Canadian Journal of Law and Technology

Volume 21 | Number 1 Article 2

7-2023

Slouching Toward Regulation: Assessing Bill 88 as a Solution for Workplace Surveillance Harms

Danielle E. Thompson
University of Waterloo, Department of Sociology and Legal Studies

Adam Molnar
University of Waterloo, Department of Sociology and Legal Studies

Slouching Toward Regulation: Assessing Bill 88 as a Solution for Workplace Surveillance Harms*

*Danielle E. Thompson*** & *Adam Molnar****

Abstract

Employee monitoring applications ("EMAs") are proliferating in Canada and provide employers with sophisticated surveillance tools for the monitoring of workers (e.g., on-device video surveillance, browser activity, and email monitoring). In response to concerns about these increasingly invasive surveillance practices, the Government of Ontario passed Bill 88, the Working for Workers Act, 2022*, which requires all employers with 25 or more workers to have a written policy stating whether and how they electronically monitor their employees. Bill 88 marks a more explict attempt to regulate workplace surveillance in a modern digital context in Canada; however; however, an analysis of the Bill's capacity as a meaningful regulatory mechanism has yet to be conducted.*

This article engages in a critical analysis of Bill 88's capacity to meaningfully protect employee privacy in a contemporary remote workplace, with particular emphasis on the emergence and use of EMAs. Specifically, we examine the multitude of harms generated by EMAs, situate Bill 88 within existing legislation and common law, identify remaining regulatory gaps within the Bill's framework, and evaluate its capacity to mitigate surveillance harms. Despite Bill 88's attempt to better inform Ontario workers about the electronic monitoring practices of their employers, in its current form, we argue that the bill is an incomplete and ineffective comprehensive regulatory solution for EMAs. The primary objective of Bill 88, to enhance transparency, and the Bill's framing of workplace surveillance harms through the lens of "individual privacy," limit more meaningful regulatory interventions that might otherwise address the harm-generating mechanisms of EMAs themselves.

We recommend that Bill 88 be meaningfully amended to (a) consider the numerous impacts of workplace surveillance that extend beyond a narrow privacy framework (e.g., social, psychological), (b) place restrictions on employers on when, where, and how EMAs can be used, and (c) afford workers with the right to

---

* This publication draws on research supported by the Social Sciences and Humanities Research Council. Cette publication s'appuie sur des recherches soutenues par le Conseil de recherches en sciences humaines.

** Danielle E. Thompson is a PhD Candidate in the Department of Sociology and Legal Studies at the University of Waterloo, where she is also a member of the student advisory committee for the Waterloo Cybersecurity and Privacy Institute.

*** Adam Molnar is Assistant Professor of Sociology and Legal Studies at the University of Waterloo, where he is also an executive member of the Waterloo Cybersecurity and Privacy Institute.

file complaints related to the necessity and proportionality of EMA use by employers.

Résumé

Les applications de surveillance des employés (« EMA ») prolifèrent au Canada et fournissent aux employeurs des outils de surveillance sophistiqués pour la surveillance des travailleurs (par exemple, la surveillance vidéo sur l'appareil, l'activité du navigateur et la surveillance des courriels). En réponse aux préoccupations concernant ces pratiques de surveillance de plus en plus envahissantes, le gouvernement de l'Ontario a adopté le projet de loi 88, la Loi de 2022 sur le travail pour les travailleurs, qui oblige tous les employeurs de 25 travailleurs ou plus à avoir une politique écrite indiquant s'ils surveillent électroniquement leurs employés et comment ils le font. Le projet de loi 88 marque une tentative plus explicite de réglementer la surveillance en milieu travail dans un contexte numérique moderne au Canada; cependant, une analyse de la capacité du projet de loi en tant que mécanisme de réglementation significatif n'a pas encore été menée.

Cet article s'engage dans une analyse critique de la capacité du projet de loi 88 à protéger de manière significative la vie privée des employés dans un lieu de travail contemporain à distance, avec un accent particulier sur l'émergence et l'utilisation des EMA. Plus précisément, nous examinons la multitude de méfaits générés par les EMA, situons le projet de loi 88 dans la législation existante et la common law, identifions les lacunes réglementaires restantes dans le cadre du projet de loi et évaluons sa capacité à atténuer les méfaits de la surveillance. Malgré la tentative du projet de loi 88 de mieux informer les travailleurs ontariens sur les pratiques de surveillance électronique de leurs employeurs, dans sa forme actuelle, nous soutenons que le projet de loi est une solution réglementaire complète incomplète et inefficace pour les EMA. L'objectif principal du projet de loi 88, à savoir améliorer la transparence, et le cadre du projet de loi sur les méfaits de la surveillance du lieu de travail à travers le prisme de la «vie privée individuelle», limitent les interventions réglementaires plus significatives qui pourraient autrement s'attaquer aux mécanismes générateurs de préjudices des EMA elles-mêmes.

Nous recommandons que le projet de loi 88 soit modifié de manière significative pour (a) tenir compte des nombreux impacts de la surveillance du lieu de travail qui vont au-delà d'un cadre étroit de confidentialité (par exemple, social, psychologique, etc.), (b) imposer des restrictions aux employeurs sur le moment, le lieu et comment les EMA peuvent être utilisées, et (c) donner aux travailleurs le droit de déposer des plaintes liées à la nécessité et à la proportionnalité de l'utilisation de l'EMA par les employeurs.

INTRODUCTION

Since the onset of the Covid-19 pandemic, employee monitoring applications have been at the forefront of government, media, and scholarly conversations as

Canadians question what constitutes *too much* surveillance in the workplace.[1] Employee monitoring applications (''EMAs'') are a type of digital surveillance software that enables employers to remotely monitor the behaviour of their workers, making them particularly salient in the era of ''remote work.'' These applications (e.g., Kickidler, ActivTrak, or Teramind) provide companies with a toolkit of advanced surveillance mechanisms, such as keystroke logging, webcam video surveillance, desktop screenshots, and email monitoring,[2] that significantly increases the capacity of employers to monitor workers.[3] Since the Covid-19 pandemic in March 2020 and the associated pivot to ''remote work,'' the global demand for EMAs has risen sharply compared to the previous year, with adoption increasing by 108% and vendor sales enquiries at two notable companies increasing by 169% (Teramind) and 139% (Kickidler), respectively.[4] While companies view monitoring software as a helpful remote management tool that allows them to ''limit cost and risk, protect value and maintain quality,''[5] the global influx of EMAs into home environments blurs conventional work-home boundaries and raises serious questions about privacy rights related to the workplace and the protection of professional and personal lives from employer surveillance.

Legal scholars have long examined the delicate balance that exists between legitimate forms of employee monitoring and workers' rights to privacy from workplace surveillance.[6] While existing literature, although outdated, does suggest Canada recognizes privacy rights in the workplace[7] — a notion that was further underscored by *R. v. Cole*[8] — Canada's regulatory landscape is argued to be uneven and to resemble a ''patchwork quilt.''[9] Federally regulated workers

---

1 See e.g., New York Times, ''The Rise of Workplace Surveillance'' (2022), online (podcast): *The Daily* < podcasts.apple.com/ca/podcast/the-rise-of-workplace-surveillance/id1200361736?i = 1000577192855 > [NYT Podcast].

2 Kirstie Ball, *Electronic monitoring and surveillance in the workplace: Literature review and policy recommendations* (Luxembourg: Publications Office of the European Union, 2021).

3 Daniel Ravid et al,''EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring'' (2020) 46:1 J Management 100 at 101.

4 Ball, *supra* note 2.

5 Jijo James Indiparambil, ''Privacy and Beyond: Socio-Ethical Concerns of 'On-the-Job' Surveillance'' (2019) 8:1 Asian J Bus Ethics 73 at 80.

6 Avner Levin, ''Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada'' (2007) 22:2 CJLS 197; Graeme Lockwood & Vandana Nath, ''The Monitoring of Tele-Homeworkers in the UK: Legal and Managerial Implications'' (2021) 63:4 Intl JL & Management 396.

7 Melanie Bueckert, ''Electronic Employee Monitoring: Potential Reform Options'' (2009) 6 Man LJ 99; Michael Geist, ''Computer and E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance'' (2003) 82:2 Can Bar Rev 151.

8 *R. v. Cole*, 2012 SCC 53, 2012 CarswellOnt 12684, 2012 CarswellOnt 12685 (S.C.C.).

9 Levin, *supra* note 6 at 198.

(e.g., airlines) are governed by federal legislation known as the *Personal Information and Electronic Documents Act* ("PIPEDA"). Provincial privacy legislation that deals with personal information within the workplace exists within the provinces of Quebec (*An Act Respecting the Protection of Personal Information in the Private Sector*), British Columbia, and Alberta (*Personal Information Protection Act*); however, certain jurisdictions, such as Ontario, are not "subject to any legislation at all."[10]

In response to these concerns, on April 11, 2022, the Government of Ontario passed Bill 88, *the Working for Workers Act*, *2022*, which seeks to protect digital workers' privacy by requiring companies to be transparent in their employee monitoring practices.[11] Schedule 2 of Bill 88 makes amendments to the *Employment Standards Act, 2000* by requiring all employers with 25 or more workers to have a written policy stating whether and how they electronically monitor their employees, including "a description of how and in what circumstances the employer may electronically monitor employees, and the purposes for which information obtained through electronic monitoring may be used by the employer."[12] Under Bill 88, companies are required to provide workers with a written electronic monitoring policy no later than 30 days after the policy's creation and amendment or the employee's hiring date. Employees have the right to complain to the Minister of Labour, Training and Skills Development if the policy is not provided by the employer within these timelines.[13]

Bill 88 marks the first formal attempt of EMA regulation within the Canadian context. As such, it exists as a benchmark for EMA legislation and regulation nation-wide. In spite of this, an analysis of the Bill's capacity as a meaningful safeguard within a broader web of regulatory measures has yet to be conducted, leaving academics, the legal community, employers, and employees with many unanswered questions. How does Bill 88 protect worker privacy, both in terms of legislation, but especially in terms of practice? Are there any regulatory gaps involving Bill 88 and its broader legal context for the regulation of EMAs? And is there a different regulatory approach that may be equally, if not more, meaningful for the protection of worker privacy in a post-Covid world? Particularly one that is characterized by a remote work environment. The

---

10 *Ibid.*

11 Bill 88, *An Act to enact the Digital Platform Workers' Rights Act, 2022 and to amend various Acts*, 2nd Sess, 42nd Leg, Ontario, 2022 (assented to 11 April 2022), SO 2022, c 7; Letter from Patricia Kosseim, Information and Privacy Commissioner of Ontario, to Natalia Kusendova, Chair of the Standing Committee on Social Policy (14 March 2022), "RE: Schedule 2 of Bill 88, the Working for Workers Act, 2022," online (pdf): <www.ipc.on.ca/wp-content/uploads/2022/03/2022-03-14-ltr-standing-committee-on-social-policy-re-schedule-2-of-bill-88-the-working-for-workers-act-2022.pdf> [Kosseim, RE: Schedule 2 of Bill 88].

12 Bill 88, *An Act to Enact the Digital Platform Workers' Rights Act, 2022 and to Amend Various Acts*, 2nd Sess, 42nd Leg, Ontario, 2022.

13 *Ibid*; Kosseim, "RE: Schedule 2 of Bill 88," *supra* note 11.

following article considers the extent to which Bill 88 meaningfully protects employee privacy in a contemporary remote workplace, with particular emphasis on the emergence and use of EMAs. While measures that claim to address power imbalances between employers and employees created by technical innovations are an important first step for addressing labour rights in the digital workplace, failure to meaningfully protect privacy comes at the cost of appearing to do so. The implications of our analysis are relevant for the scholarly and legal communities, policy-makers, regulators, and a range of labour and civil society organizations interested in the practical outcomes of early attempts to address privacy considerations in a post-Covid context.

Part 1 of this article provides an overview of the existing features, uses, and harms of EMAs, laying the groundwork for our analysis of the harmful implications of these technologies and the competency of existing regulatory mechanisms. Such a consideration of the development of workplace surveillance technologies, and how increasingly powerful and invasive these technologies have become, also invites the opportunity to revisit relevant statutory and common law decisions and to assess their capacity to mitigate surveillance-related harms (something that we will turn to in Part 3). Part 2 draws upon the idea of the "technology-harm nexus"[14] to gain a deeper understanding of the specific constellation of harms generated by digital monitoring technologies, and EMAs in particular, in the modern workplace. Drawing on the work of Brownsword,[15] Part 3 elaborates on the specific details of Bill 88 within the broader regulatory web governing workplace surveillance in Canada and considers how the legislation is framed as a meaningful solution to EMAs. Part 4 engages in a critical analysis of whether Bill 88 effectively mitigates the harms generated by EMAs and identifies existing gaps — what Brownsword calls "regulatory disconnect"[16] — in the Bill's regulatory framework. Consideration is also given to the problematic framing of EMA harms as an individual privacy issue rather than a surveillance-related harm. Part V concludes with a discussion of recommendations for a more meaningful amendment of Bill 88.

1. WORKPLACE SURVEILLANCE, EMPLOYEE MONITORING, AND WORKER RIGHTS TO PRIVACY

Many advancements have been made in workplace surveillance technologies since the early days of workplace monitoring.[17] Employee monitoring, which previously occurred strictly through physical observation by supervisors for "performance control of subordinates," now also operates electronically where

---

[14] Mark Wood, "Rethinking How Technologies Harm" (2021) 61:3 Brit J Crim 627.

[15] Roger Brownsword, *Law 3.0: Rules, Regulation, and Technology* (New York: Routledge, 2019).

[16] *Ibid.*

[17] See e.g., Ball, *supra* note 2.

"digital systems are used to track employee performance and behaviour."[18] An adequate grasp of the distinct technological features of these systems and their applied uses is crucial for understanding the ways in which these systems are implicated in workplace harms and how they are (or are not) accounted for in existing regulatory mechanisms. The value and legitimacy of workplace surveillance is argued to be based on whether technologies act as tools for managers to *care* for the interests of their employees or as "powerful instrument(s) of managerial *coercion* and employee subordination" (*emphasis added*)[19]. The latter rationale is arguably prominent in the use of EMAs by organizations. While the occupational safety/care rationale seeks to ensure the wellbeing of employees (e.g., through the use of sensor data to track physiological conditions or adverse ergonomic movements), the control/coercion rationale centers on ensuring company security (e.g., preventing unauthorized sharing of trade secrets), increasing economic efficiency, and tracking other deviant behaviours (e.g., private internet use on company time).[20] According to Ravid et al's four-part typology of electronic performance monitoring,[21] dominant rationales for the adoption of monitoring tools are broken down into four categories: (a) performance focused (i.e., for performance appraisals, loss prevention, profit), (b) development focused (i.e., for development, growth, training), (c) administration and safety focused (i.e., for protection from legal or civil harm), and (d) surveillance and control focused (i.e., for monitoring without explicit reason). Coercive or controlling forms of surveillance are furthered through the proliferation of digital monitoring technologies which extend employer surveillance "beyond the realm of performance management and into the behaviours and personal characteristics of the employee."[22] Employers now have the capacity to do the following:

> ... broadcast and record employee desktop activity online in real time, take screenshots of employees' desktops remotely, track the time employees spend working, nudging them if they are not, detect whether they are engaging in negligent or illegal activities and generate both individual and departmental performance metrics, and behaviour analytics among other things.[23]

This new type of surveillance for remote workers relies on a different form of performance measurement that bases assessments on behaviour measures (i.e., adherence to task level prescriptions) rather than output controls (i.e., successful

---

[18] Nils Backhaus, "Context Sensitive Technologies and Electronic Employee Monitoring: a Meta-Analytic Review" (Proceedings of the 2019 IEEE/SICE International Symposium on System Integration, Paris, France, 14 — 16 January 2019) at 548.

[19] Indiparambil, *supra* note 5 at 78.

[20] Backhaus, *supra* note 18.

[21] Ravid et al, *supra* note 3.

[22] Ball, *supra* note 2 at 11.

[23] *Ibid* at 54.

target achievement).[24] As such, it relies on the extensive collection of detailed personal data about employee's behaviour in striking ways. Employer reliance on data intended to reflect behavioural measures incentivizes frequent and intrusive monitoring, reduces worker autonomy, and is more likely to be perceived as excessive by workers.[25]

EMAs have been deemed "one of the biggest expansions of employer power in generations,"[26] and, according to scholars Lockwood and Nath,[27] employees have limited protections under the law[28] and "face fears of total surveillance and the loss of privacy and freedom at work."[29] The monitoring of worker communications (i.e., phone, internet, and social media activity) is argued to be "one of the most common, yet highly controversial" types of employee surveillance.[30] The issue of near-persistent and detailed collection of data is further complicated by the overlaps between personal devices and company-sponsored devices for both work and private activities. Employers routinely monitor and discipline workers for inappropriate social media use as well as private video or images detected through the camera of the device. For example, judgements may be made about the "appropriateness" of an employee's work environment, yet background images or noises may be considered unprofessional or inappropriate, and be "erroneously linked to work performance issues."[31] Remote workers, therefore, must be extremely careful about the "seepage" of private matters into the work realm[32] — which, in the case of remote workers, involves any activities, conversations, or background imagery that can be captured within the frame of video surveillance technologies. The rapid advancement of workplace surveillance and the increasingly invasive nature of these technologies, particularly in their capacity to permeate boundaries that previously existed between work and home spaces, has foregrounded concerns related to the impacts of these technologies on employee privacy.

Privacy, as a theoretical framework and legal-normative order, is often the primary consideration when assessing the impacts of surveillance. While various definitions exist within the literature, there is general agreement that the term privacy "denotes a state of being free from unwanted intrusion or disturbance in one's life and affairs."[33] Seven types of privacy are commonly identified in the

---

[24] Steven Richardson & David Mackinnon, "Becoming Your Own Device: Self-Tracking Challenges in the Workplace" (2018) 43:3 Canadian J Sociology 265.

[25] Ball, *supra* note 2.

[26] NYT Podcast, *supra* note 1.

[27] Graeme Lockwood & Vandana Nath, "The Monitoring of Tele-Homeworkers in the UK: Legal and Managerial Implications" (2021) 63:4 Intl JL & Management 396.

[28] *Ibid.*

[29] Backhaus, *supra* note 18 at 19.

[30] Lockwood & Nath, *supra* note 27.

[31] *Ibid* at 406.

[32] *Ibid.*

surveillance literature: (1) privacy of the person, (2) privacy of personal behaviour, (3) privacy of personal data, (4) privacy of personal communication,[34] (5) privacy of thoughts and feelings, (6) privacy of location and space, and (7) privacy of association.[35] According to Wright and Raab,[36] any meaningful assessment of the impact of surveillance on privacy *must* address *all* seven types. This is paramount in the examination of EMAs, especially within the home, which may capture the occurrence of personal matters or behaviours through video recording (i.e., privacy of personal behaviours), private conversations related or unrelated to work through email monitoring (i.e., privacy of personal communication and thoughts and feelings), and information related to one's social life and relationships through social media monitoring (i.e., privacy of person and of association). The possible use of this information for disciplinary or performance purposes must also be addressed. The powerful surveillance mechanisms that are now readily available to employers, and their newfound application to the context of remote management, underscore the importance of understanding the breadth and depth of privacy invasiveness posed by EMAs.

Ravid et al help us to further clarify the extent of privacy invasion posed by EMA technologies by classifying key characteristics of privacy-invasive monitoring practices, such as electronic performance monitoring ("EPM") through EMAs.[37] Invasiveness is defined as "the intrusion that EPM poses to privacy, autonomy, or sense of personal boundaries"[38] and is composed of four sub-elements: scope, target, monitoring constraints, and employee control. First, scope describes the breadth and specificity of the data collected — that is, how much an individual is monitored and the level of inquiry upon which the data is collected. Here, performance-monitoring technologies can be utilized to collect organizational-level data without collecting specific data on employees, or it can be used in a more invasive manner to track and store data on individual employees. Second, the target refers to the type of information that is collected by the performance-monitoring technology and can vary by intimacy level (with higher degrees of intimacy indicating higher invasiveness and sensitivity of personal information). EMAs, as a performance-monitoring tool, can collect information related to (a) the thoughts, feelings, and physiology of individuals (e.g., social media, email monitoring); (b) body or location (e.g., video

---

[33] Indiparambil, *supra* note 5 at 82.

[34] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" (August 1997), as cited in David Wright & Charles Raab, "Constructing a Surveillance Impact Assessment" (2012) 28:6 Computer L & Sec Report 613.

[35] Rachel Finn, David Wright & Michael Friedewalde, "Seven Types of Privacy" in Serge Gutwirth, Ronald Leenes Paul de Hert & Yves Poullet, eds, *European Data Protection: Coming of Age* (Dordrecht: Springer, 2013) 3, as cited in *ibid* at 617.

[36] Wright & Raab, *supra* note 34.

[37] Ravid et al, *supra* note 3.

[38] *Ibid* at 108.

monitoring, GPS tracking); and (c) tasks (e.g., keystroke logging). Third, monitoring constraints encompass the "explicit limits on when and how electronic performance monitoring can occur, how data will be used, and who will have access to the data once they are collected."[39] High constraints related to EMAs would entail clear parameters on who can access the data and how it can be used (i.e., low invasiveness) or even prohibit data collection altogether. And fourth, target control describes the degree of control that monitored individuals have over the timing and mechanisms used to monitor their performance and behaviour.[40] High target control provides employees with the power to decide when and how they are monitored (e.g., allowing monitoring to be turned off when on breaks) (i.e., low invasiveness).

Ravid et al's classification system for invasive technologies is therefore beneficial for understanding the potential impacts of EMAs on employee privacy. According to this spectrum of invasiveness, EMAs can be understood as a highly privacy-invasive surveillance mechanism that collects individual-level data on employees (i.e., scope), including highly intimate data types (e.g., email monitoring, video surveillance through device cameras, biometrics, keystroke logging, etc.) (i.e., target), that is frequently used without informing employees of plans for data use and access permissions (i.e., low monitoring constraints), and that provides employees with little to no control over when and how they are monitored (i.e., low target control). If we recognize EMAs as being a highly invasive mechanism of surveillance, then reducing the negative impact of this technology on employee privacy is likely to be a chief concern — a focus that has been underscored in Bill 88. Such concerns of privacy are often mitigated through attempts to increase transparency in employer operations, as it is deemed to be important for reducing worker perceptions of EMAs as privacy invasive, for preserving worker autonomy, and for building trust.[41] Nontransparent monitoring has been found to undermine employer-employee trust relationships and to "give rise to a number of difficult legal and employee relations issues."[42] Both employers and the law are therefore faced with the challenge of balancing the desire of companies to monitor workers with the privacy rights of employees;[43] and the answer to this dilemma has most often been transparency focused. In fact, Bill 88's requirement for Ontario companies to produce an electronic monitoring policy is entirely premised on this notion of transparency. But is increased transparency in monitoring practices a sufficient regulatory mechanism on its own? And does it sufficiently mitigate the harms posed by EMA technologies?

---

[39] *Ibid* at 109.

[40] *Ibid.*

[41] Indiparambil, *supra* note 5.

[42] Lockwood & Nath, *supra* note 27 at 399.

[43] *Ibid.*

While the issue of privacy, and the ancillary solution of transparency, is one of the most evident and predominantly discussed impacts of workplace surveillance, Indiparambil argues that this near-exclusive focus on individual rights produces a tendency to overlook impacts and consequences of surveillance that extend beyond privacy.[44] Such impacts include social (e.g., discrimination or social exclusion),[45] political (e.g., impact on democratic rights such as freedom of speech and association), legal (e.g., compliance with current legislation),[46] ethical (e.g., impact on autonomy, informed consent, or justice),[47] psychological (e.g., decreased job satisfaction and increased stress levels and turnover rates),[48] and economic and financial (e.g., costs of establishing surveillance mechanisms).[49] This latter point also speaks to the potential impacts of EMAs when used as a disciplinary mechanism to ensure the extraction of relative surplus value from workers (i.e., the Marxist account of exploitation).[50] In fact, EMA usage for remote workers is quite notable in our contemporary moment for how it structurally and strategically facilitates the reappropriation of surplus value by employers, as EMAs ensure stringent control over worker productivity and efficiency, and remote working reduces company overhead. Given the pervasive characteristics of EMA-surveillance and their wide-ranging impacts, an examination of "the potentially harmful effects of surveillance on a wider basis than that of protecting privacy"[51] is required to appreciate how these effects are registered both in theoretical frameworks and in legal norms. Wright and Raab, for example, urge the use of surveillance impact assessments over assessments that focus solely on invasions of privacy, an approach that opens up considerations of the broader range of harms and societal impacts of surveillance mechanisms such as EMAs.[52] While this consideration of the broad impacts of EMAs is certainly important, it is not sufficient on its own for the successful mitigation of surveillance harms. The invasive nature of EMAs stems not only from their material properties (i.e., how they are designed) but *also* from the social and informational contexts in which they are applied. Are EMA technologies intrinsically invasive by design, or do surveillance harms emerge from how these technologies are used by employers? To gain a more comprehensive understanding of the production of surveillance harms (specifically, those emerging from the use of EMAs), we turn to the following

---

44 Indiparambil, *supra* note 5.

45 *Ibid*; Wright & Raab, *supra* note 34.

46 Lockwood & Nath, *supra* note 27; Wright & Raab, *supra* note 34.

47 *Ibid*.

48 Ball, *supra* note 2.

49 Wright and Raab, *supra* note 34.

50 Christian Fuchs, "Political Economy and Surveillance Theory" (2013) 39:5 Critical Sociology 671.

51 Surveillance Studies Network, n.d., as cited in Wright & Raab, supra note 34 at 614.

52 *Ibid*.

section, which details *how* EMA-generated surveillance harms are produced through distinct human-technology relations. Here, we argue that any successful regulatory response aimed at mitigating surveillance harms, including Bill 88, must contend with both the technical (i.e., design) *and* social (i.e., application) properties of EMA surveillance in the workplace.

2. THE TECHNOLOGY-HARM NEXUS

A comprehensive understanding of EMAs requires an examination of "the various ways in which human-technology relations are implicated in generating harmful events."[53] Wood understands surveillance technologies as "socio-technical" apparatuses that have both distinctly technical and distinctly social properties.[54] A failure to distinguish between the "social" and the "technical" undermines our ability to understand how different harm-generating mechanisms exist through configurations of social structures and technologies.[55] Recognizing how EMA-surveillance related harms are produced through discrete configurations of "social" and "technical" mechanisms is not only illuminating for grasping the ways that aspects of design *as well as* social uses and values cohere to produce harms; it also helps to clarify the design and effectiveness of existing (and proposed) regulatory solutions for the mitigation of EMA harms.

Wood's understanding of technology-harm relations is further premised on two principles, the first being that, while values are designed into technologies, the uses of technology almost always surpass those intended by its designer.[56] This allows for a crucial distinction to be made between harms that arise out of the "intended uses and effects of a technology" and harms that arise out of the "unintended uses, needs, ends, functions and mechanisms engendered by technologies."[57] The second principle acknowledges the need to understand not only what technologies afford to individuals, but also how they shape identities, interests, and beliefs. This allows for a distinction to be made between harms that are "a product of individuals intentionally using technologies to harm" where the technology provides them with the means to harm, and harms that are "a product of what technologies do *to* individuals, collectives, and/or environments."[58] Applying these principles, we can distinguish between four types of technology-harm relations:

1. technology that is both designed and used as a means to harm;

---

[53] Wood, *supra* note 14 at 628.

[54] *Ibid.*

[55] *Ibid.*

[56] *Ibid.*

[57] *Ibid* at 638.

[58] *Ibid* at 639.

2. unintended harms of technology functioning in ways unintended by designers;
3. unintended harms of technology functioning as intended by designers; and,
4. harms resulting from the intentional use of technology for harmful purposes not intended by designers.

The majority of EMA harms discussed within Part I of this article can be classified as unintended harms of technology functioning as intended, including invasions of worker privacy, autonomy, and freedom; erosion of trust; and a weakening of employer-employee relations. These effects are vastly different from those marketed by EMA software vendors. Consider ActivTrak, one of the top ten EMAs used by Canadian businesses,[59] which markets their software as providing businesses with the tools to "empower your people, hone healthy work habits, and optimize processes so you can do great things"[60] — a far cry from eroding worker trust, autonomy, and freedom. While the above harms produced by EMAs do appear to be unintended, what must be emphasized here is that these harms are generated from the software *functioning as intended*. Indeed, a smaller number of harms can be classified as harms where EMAs are intentionally used by employers for harmful purposes in a way that was not envisioned by the designers. An example of this may include the capturing of scenery, activities, and conversations occurring in the background of a remote worker's video camera frame and the use of this information by employers in performance reviews or for disciplinary purposes. While this type of harm does occur, and is made possible through the use of EMAs, a large majority of the harms generated by EMAs are not due to technology misuse or abuse, but rather a result of the software *functioning as intended* by designers. This is a noteworthy conclusion that adds urgency to understanding whether existing legislation is suitable to mitigate the types of surveillance harms generated by EMAs.

3. MOVING FROM LAW 1.0 TO LAW 2.0

Prior to the establishment of Bill 88, existing legislation that protected the privacy rights of Ontarians consisted of the *Freedom of Information and Protection of Privacy Act, 1990* ("FIPPA"), the *Municipal Freedom of Information and Protection of Privacy Act, 1990* ("MFIPPA"), and the *Personal Health Information Protection Act, 2004* ("PHIPA"). While FIPPA and MFIPPA are intended to protect the privacy of personal information collected and retained by institutions, these Acts do not apply to "most employment-related and labour relations information."[61] PHIPA therefore

---

[59] Thompson and Molnar, "Workplace Surveillance in Canada: A survey on the adoption and use of employee monitoring applications" (Forthcoming) Canadian Review of Sociology.

[60] ActivTrak, "Workforce Analytics for the Modern Workplace" (2022), online: <www.activtrak.com>.

marks the only provincial legislation within Ontario that protects employee privacy rights; however, the Act applies only to workplaces that handle private health information. Additional Ontario laws that govern the rights of employees in the workplace, such as the *Employment Standards Act, 2000* and the *Labour Relations Act, 1995*, prior to Bill 88, did not previously address employee privacy rights or protections from employer surveillance. There was therefore no existing legislation in Ontario that was suitable for the regulation of EMAs and the protection of employees from employer surveillance. The legal and regulatory web governing workplace surveillance in Ontario, however, extends beyond provincial and federal legislation to include relevant common law (including contracts of employment and tort remedies), as well as a quasi-constitutional right to privacy in s 8 of the *Charter of Rights and Freedoms*.

Three major judicial decisions are pertinent to understanding issues of workplace surveillance: *R. v. Cole,*[62] *Jones v. Tsige,*[63] and *Bhasin v. Hrynew*.[64] In terms of the constitutional right to privacy, in *R. v. Cole*, the court determined that employees maintain a reasonable expectation of privacy at work even when using employer-owned devices. In this case, an IT administrator employed by the school board discovered nude images of an underage student on the teacher's school-board-issued laptop and reported the images to the principal of the school. The school copied some of the materials and provided the device to the police, who then conducted a warrantless search of the device. The school board's electronic device policy maintained that the computer was for work purposes and that only "incidental personal use" was allowed.[65] In spite of this documented policy, in practice, the school permitted personal use. The accused used the device in line with these generally accepted practices,[66] storing personal information on the device, including family photographs. While an initial search of the device by the school board, a public employer, was implicitly authorized by the *Education Act* (which requires the maintenance of a safe school environment),[67] the court ultimately determined that the teacher had a reasonable expectation of privacy from the police (for criminal investigative purposes) in the contents stored on the device. Because the search of this information took place without a warrant, it was deemed to be presumptively unreasonable and a violation of s 8 of the *Charter*.[68] The decision of *R. v. Cole* is

---

[61] Ontario Government, "Privacy Protection" (2019), online: <www.ontario.ca/document/freedom-information-and-privacy-manual/privacy-protection>.

[62] 2012 SCC 53, 2012 CarswellOnt 12684, 2012 CarswellOnt 12685 (S.C.C.) [*Cole*].

[63] 2012 ONCA 32, 2012 CarswellOnt 274 (Ont. C.A.).

[64] 2014 SCC 71, 2014 CarswellAlta 2046, 2014 CarswellAlta 2047 (S.C.C.).

[65] *Cole*, *supra* note 62 at para 16.

[66] *Ibid* at para 54.

[67] *Education Act*, RSO 1990, C E.2, s 265.

[68] *Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc.*, 1984 CarswellAlta 121, 1984 CarswellAlta 415, (*sub nom.* Hunter v.

important in two ways. First, it reaffirmed the right to privacy in Canada, moving away from a property-based conception of privacy and toward one that is further rooted in informational privacy and a person's biographical core.[69] And second, it reaffirmed that the school board's authority to search the board-owned device does not extend to authorizing a subsequent search by police for criminal investigative purposes, thereby maintaining the principle that a third party cannot undermine another's privacy rights (i.e., it further rejected the third-party doctrine). The implications of *R. v. Cole* for workplace monitoring is straightforward: individuals have a reasonable expectation of privacy in their personal information (which extends to work-issued devices), but these protections against unreasonable search from the state does not necessarily extend as a protection from one's own employer.[70]

In terms of common law, tort remedies and contracts of employment are relevant for shaping conditions of workplace surveillance. In *Jones v. Tsige*, the Court of Appeal for Ontario recognized a right of action for the tort of "intrusion upon seclusion"[71] that can have consequences for digital privacy in the workplace. The defendant in *Jones v. Tsige* was an employee at a bank who used their work device to intentionally access the plaintiff's personal banking information at least 174 times over four years. While the defendant and the plaintiff did not know one another, the defendant was in a common law relationship with the plaintiff's former husband. There was no legitimate work-related purpose for the defendant to access the plaintiff's financial information; rather, the defendant stated that her access to the records was in relation to a financial dispute she was having with her ex-husband over child support payments. In a unanimous ruling, the panel established a tort of "intrusion upon seclusion" to include a "right to informational privacy."[72] According to the Ontario Court of Appeal, the intrusion upon seclusion tort is constituted on the basis of three elements:

1. the conduct of the defendant was intentional or reckless;
2. the defendant invaded, without lawful justification, the plaintiff's private affairs or concerns; and,

---

Southam Inc.) [1984] 2 S.C.R. 145 (S.C.C.); *R. v. Nolet*, 2010 SCC 24, 2010 CarswellSask 368, 2010 CarswellSask 369 (S.C.C.) at para. 21; *R. v. Collins*, 1987 CarswellBC 94, 1987 CarswellBC 699, (*sub nom.* Collins v. R.) 38 D.L.R. (4th) 508, [1987] 1 S.C.R. 265 (S.C.C.).

69 Karen Eltis, "Piecing Together Jones, A.B. and Cole: Towards a 'Proportional' Model of Shared Accountability in Workplace Privacy" (2015) 18:2 CLELJ 493 at 508.

70 It is also worth noting, however, that while s 8 considerations focus on informational privacy and the "biographical core," the Ontario Court of Appeal has affirmed that s 8 can also "protect informational privacy interests beyond that 'biographical core'" (see *R. v. Orlandis-Habsburgo*, 2017 ONCA 649, 2017 CarswellOnt 12187 (Ont. C.A.) at para. 79).

71 *Supra* note 63.

72 *Ibid* at para 66.

3. a reasonable person would regard the invasion as highly offensive, causing distress, humiliation, or anguish (considering the degree, context, conduct, and circumstances of the intrusion).[73]

The court took care to note that proving economic damages was not a required element of the cause of action, holding that the plaintiff could be entitled to "symbolic" or "moral" damages that are designed to "vindicate rights or symbolize recognition of their infringement."[74] In *Jones v. Tsige*, the Court of Appeal awarded the plaintiff $10,000 in damages, while setting the range of available moral damages for the tort "at up to $20,000." Reliance on the tort of intrusion upon seclusion in workplace surveillance faces practical limitations. First, it relies on a plaintiff (an employee) being aware that the defendant (an employer) has indeed invaded the employee's individual affairs. It could be argued that, while most workers that are subject to EMAs *may* be aware that their behaviours are being monitored, they may not fully know the extent of this surveillance, including whether it extends to parts of their devices that contain sensitive personal information (such as health and financial records). Indeed, with the use of third-party software to facilitate the surveillance, even employers may be unaware of the scope and sensitivity of the data that is collected on their employees and how it might transit the internet.

And finally, the courts have recognized a common law duty that applies to the application of contracts in Canada. Since the precedent-setting SCC case *Hrynew*,[75] courts have recognized a duty that discretion is exercised according to the organizing principle of good faith. The court's decision in *Hrynew* determined that parties to an employment contract must perform their contractual duties honestly and reasonably, recognizing and acting in line with each party's legitimate interests. Through agreement, contracting parties may determine the criteria through which the performance of contractual obligations is to be measured, but only insofar as they adhere to minimum requirements of honest performance. Notably, while the application of a good faith organizing principle to contractual performance is to be applied contextually, with multiple factors being involved, it is largely recognized that there may be a trend toward a potential duty to conduct managerial prerogatives with good faith. Put differently, a court's recognition of an act of bad faith by an employer may be a remedy for an employee who is not otherwise legally entitled to an award of monetary damages. Like the aforementioned tort of intrusion upon seclusion, violations of contracts depend on the discovery that a violation has occurred in a notoriously non-transparent environment.

Additionally, the role of collective bargaining in the digitized workplace has led to some union-negotiated protections contained within common law contracts of employment. While empirical research on the extent to which

---

[73] *Ibid* at para 71.

[74] *Ibid* at para 75.

[75] *Supra* note 64.

trade unions in Canada have incorporated concerns about privacy into their collective agreements is both sparse and outdated,[76] represented in Canadian collective agreements under federal and provincial labour laws (76 out of 5,495).[77] In spite of the absence of a much-needed update of this literature, we can still infer that collective bargaining presents a valuable opportunity to shape the definition, purpose, scope, and transparency of electronic monitoring in the workplace. The efficacy of union-negotiated protections from surveillance-related harms is, however, dependent on the robustness of unions more generally. As such, the limited protections that exist via union-negotiated contracts are likely to be very unevenly distributed based on the sector (public vs private) and on the extent to which a sector leans toward occupations relating to intellectual property and freedom of expression, such as the post-secondary sector and media. While union-negotiated protections appear promising in principle, their practical limitations are no substitute for broadly applicable statutory protections.

It is within this regulatory web that we see the emergence of Bill 88 (and the movement from Law 1.0 to Law 2.0): new technologies such as EMAs may not be comprehensively regulated by existing laws and consequently force the development of new legislation. The emergence of Bill 88 to fill an existing regulatory gap therefore reflects two key concepts presented by Brownsword[78] that describe the challenges of regulating technological innovations. Brownsword uses the term "Law 1.0" to describe an initial response to technological innovation that involves "applying the general principles of the law (and its more particular rules) to specified fact situations."[79] When the limits of existing laws are reached and their adequacy to manage harm are questioned, we see the emergence of "Law 2.0." Law 2.0 requires a shift away from the courts, where principles of existing laws are applied, and into "the political arena where governments operate through the executive and legislative assemblies."[80] According to Brownsword, a Law 2.0 conversation:

> ... is not about the internal coherence or the application of general legal principles but about whether the rules are fit for purpose in responding to emerging technologies. On the one hand, the rules will be unfit if they

---

[76] Susan Bryant, "Electronic Surveillance in the Workplace" (1995) 20:4 Can J Communication 505; Simon Kiss & Vincent Mosco, "Negotiating Electronic Surveillance in the Workplace" (2006) 30:4 Can J Communication 549.

[77] *Ibid*; see also Rachel Aleks et al., "The Role of Collective Cargaining in the Digitized Workplace" in Dionne Pohler, ed, *Reimagining the Governance of Work and Employment* (Cornell University Press, 2020); given the advances in technological innovations in workplace monitoring since Kiss and Mosco's 2006 study, further research is sorely needed on the presence of surveillance- and privacy-related clauses in collective agreements in Canada.

[78] Brownsword, *supra* note 15.

[79] *Ibid* at 13.

[80] *Ibid* at 3.

> involve over-regulation, stifling the development and application of beneficial new technologies, but on the other hand, the rules will be unfit if they involve under-regulation, exposing persons to unacceptable risks (whether of a physical, psychological, financial, or other nature) or compromise values that are important in the community.[81]

The latter description of under-regulation most accurately reflects the emergence of Bill 88, which seeks to mitigate the privacy-related harms experienced by workers due to an uneven patchwork of existing (and suitable) legislation for the regulation of EMA usage in the workplace.

While Bill 88 is introduced to remedy the limits of Law 1.0, can it be said that it effectively mitigates the harms generated by EMAs? The stated primary policy objective underpinning Bill 88 is to protect workers' privacy by enhancing transparency.[82] The Act requires employers with 25 or more employees to create and provide workers with a policy outlining their use of EMAs; the Ontario Government anticipates this notification regime will better educate Ontarians on the monitoring practices in their workplace. A better awareness of EMA practices amongst workers may serve to build trust relations between employers and employees, reduce negative perceptions of EMAs as being privacy invasive, and increase perceptions of autonomy among workers;[83] however, as will be further discussed in the following section on regulatory gaps, Bill 88 only holds the potential to improve *perceptions* of trust and autonomy and does not meaningfully provide workers with increased autonomy, nor does it directly target harm-producing mechanisms. Bill 88 does, however, provide employees a right to put forward complaints to the Minister of Labour, Training, and Skills Development if their employer does not provide them with an EMA policy (but there is no such right for other harms related to necessity, proportionality, or violations of law). The Ontario Government expects this to increase perceptions of autonomy by indicating that "workers remain in the driver's seat"[84] and have some say (i.e., control) in how their behaviour is monitored. This assertion, of course, only applies insofar as other protections already exist in law. While Bill 88's pledge of protecting worker privacy through increased transparency is certainly a step in the right direction and addresses at least part of the gaps and limits in the existing patchwork of Law 1.0, there remains regulatory disconnect between the harms generated by EMAs and the proposed regulatory solution — as it stands, Bill 88 is not sufficient.

---

[81] *Ibid* at 21.

[82] Kosseim, "RE: Schedule 2 of Bill 88," *supra* note 11.

[83] Indiparambil, *supra* note 5; Lockwood & Nath, *supra* note 6.

[84] Labour, Training and Skills Development, "Ontario Requiring Employers to Disclose Electronic Monitoring" (2022): *Ontario Government* <news.ontario.ca/en/release/1001654/ontario-requiring-employers-to-disclose-electronic-monitoring>.

4. REGULATORY GAPS OF BILL 88

In its current form, Bill 88 cannot adequately mitigate the harms produced from the under-regulation of EMAs. While Bill 88 addresses an important limitation of existing legislation in that it establishes a statutory obligation to provide notification of the surveillance mechanisms used within a workplace, it only serves to increase the transparency of EMA usage by requiring employers to inform workers that they are being monitored, how the monitoring occurs, and for what purposes the data is used; it does not directly target harm-generating mechanisms. For example, in the previous section we discussed the ability of employees to submit complaints to the Minister if they are not provided with an EMA policy by their employer. This right is intended to increase transparency and instill feelings of autonomy in workers. However, the legislation does not actually afford workers what Ravid et al describe as "high target control," or the power to decide when and how they are monitored.[85] Bill 88 does not provide workers with the right to choose which surveillance mechanisms are used to monitor their work nor the right to turn off surveillance mechanisms when engaging in personal activities outside of working hours (e.g., sending personal emails when on break or after work hours) or during sensitive and private matters (e.g., turning off video surveillance if a private family matter occurs during working hours). The passing of Bill 27, *Working for Workers Act, 2021*, which provides workers with the "right to disconnect" from work-related activities outside of working hours, suggests that Ontario acknowledges the importance of work-life separation in a remote-working era;[86] however, this Bill does not explicitly address worker rights to disconnect from electronic monitoring technologies. Affording workers these rights is crucial in a remote working world where electronic devices are increasingly used for both work and personal activities.

Bill 88 also does not grant workers the right to complain to the Minister about overly invasive or excessive forms of monitoring by their employers nor the right to have those incidents investigated. Providing employees with an EMA policy is not the same as providing employees with the choice of whether, or in what ways, they are to be monitored. Employees who do not want to be monitored have to choose between losing their job or being subjected to unwanted surveillance, and, for many workers, unemployment is not a feasible option. The transparency-focused framework of Bill 88 produces an appearance of worker autonomy and control but does not actually provide workers with target control (i.e., the degree of control that a monitored individual has over the timing of the monitoring and the mechanisms used) nor does it reduce the invasive nature of monitoring applications. The latter would require a direct regulatory targeting of technology-specific harm-generating mechanisms. To be

---

[85] Ravid et al, *supra* note 3.

[86] Bill 27, *An Act to amend various statutes with respect to employment and labour and other* matters, 2nd Sess, 42nd Leg, Ontario, 2021.

clear, codifying a "right-to-know" about electronic monitoring in the workplace is a qualitative improvement from no notification requirement at all: it goes a fraction of the way to revealing that a tort violation of intrusion upon seclusion may be at play. It does not, however, mitigate the broader corrosive aspects of workplace surveillance that otherwise adhere to regulatory requirements and that are deemed "legitimate."

We know that most EMA harms result from the software operating as it was intended. In other words, most companies are *not* misusing the surveillance mechanisms afforded by EMAs; rather, these mechanisms are simply invasive *by design*. While increasing transparency will certainly make workers more aware of the existence and use of these invasive mechanisms, it will not reduce their invasive nature. Bill 88 does not place any restrictions on EMA vendors, such as a restriction on the marketing and sale of invasive (and potentially insecure) surveillance technologies in Ontario, nor does it impose any obligations for vendor transparency in the design and functioning of these mechanisms. Bill 88 also does not place any restrictions on Ontario employers regarding what purposes surveillance can be used for (e.g., cybersecurity or productivity), the types of surveillance mechanisms that are permitted for use (i.e., low invasiveness), and how data should be stored (i.e., to protect privacy of data). Bill 88 therefore sidesteps the vast array of harms that result when EMAs are used as their design intended, such as invasions of worker privacy, autonomy, and freedom. The failure to consider the storage of EMA data also raises additional concerns related to employee privacy and data anonymity, including the potential social, psychological, and economic repercussions that employees could experience if that data were to get into the wrong hands. In fact, it is entirely possible that, given the potential for EMAs to introduce security weaknesses into business and personal communication networks, they can raise a number of secondary privacy risks for consumers as well as employees that may undermine relevant statutory obligations for safeguarding consumer data required by PIPEDA. The Ontario Court of Appeal, however, has recently ruled out the availability of a tort of intrusion upon seclusion where data breaches occur as the result of malicious third-party hacking.[87] While a company may be liable under a non-privacy tort of negligence or breach of contract in using insecure EMA software, this scenario does not rise to the level of intention under the tort of intrusion upon seclusion.

Concerning data usage, Part XI.1, Written Policy on Employee Monitoring, Subsection 7 of Bill 88 reads, "For greater certainty, nothing in this section affects or limits an employer's ability to use information obtained through electronic monitoring of its employees."[88] Because Bill 88 does not restrict how

---

[87] Kate Genest, David Krebs & Amanda Cutinha, "Failure to Prevent a Data Breach Not Equal to Invasion of Privacy: Ontario Court of Appeal Shuts Door on 'Intrusion Upon Seclusion' Tort" (2 December 2022), online: <www.lexology.com/library/detail.aspx?g=0b755a46-1fc5-4839-8c56-a92dd8a84a5c>.

[88] Bill 88, *supra* note 11 at 31.

employers can use EMA data (e.g., productivity analyses), it therefore also fails to make explicit limitations on other harmful uses of EMAs by employers. Workers therefore receive no additional protections against the collection of personal or private data through employer surveillance or against the use of EMA data for performance reviews or disciplinary purposes, which can even include dismissal, beyond the existing status quo.

Much of our discussion thus far has centered around this notion of the invasion of employee privacy as the inevitable consequence of employer surveillance. Bill 88 is undoubtedly built on a privacy-centric framework — it incorporates the dominant language of privacy within the legislation. Bill 88's framing of workplace surveillance harms as an *individual* privacy issue presents a narrow conceptualization of privacy. Privacy scholars have sought to diversify understandings of privacy and move away from individualistic notions of privacy as "the protection of the self, from the state, from organizations and from other individuals"[89] toward broader conceptions that are "sensitive to the larger social issues."[90] Bill 88's objective of protecting the privacy of workers from employer surveillance misses an opportunity to codify a richer understanding of what constitutes privacy in the modern workplace and what regulatory mechanisms might meaningfully maintain it. This tendency is further illustrated through the privacy-focused solutions proposed by Bill 88, which do not encompass all types of privacy that are important to surveillance-related harms. It excludes privacy of personal behaviour (e.g., there is no restriction of invasive mechanisms such as video recording that captures behaviours and activities of employees and their families at home), privacy of personal data (e.g., there are no regulations related to how EMA data should be stored by employers), privacy of personal communication (e.g., there is no restriction of invasive mechanisms such as email monitoring that captures worker communications), privacy of location and space (e.g., there is no restriction on the use of invasive mechanisms such as GPS location trackers), privacy of thoughts and feelings, and privacy of association (e.g., there is no distinction when browser tracking or keystroke logging through EMAs cross over into private behaviour).[91] Futhermore, Bill 88's individualistic understanding of "privacy of the person"[92] as requiring protection from organizations has streamlined its regulatory approach toward organization-level solutions, such as increasing employer transparency, and away from solutions that focus on the regulation of the technology itself (e.g., regulating the use of highly invasive surveillance mechanisms or establishing parameters on activities such as video surveillance in the home). This is not to say that privacy

---

[89] Colin Bennett, "In Defence of Privacy: The Concept and the Regime" (2011) 8:4 Surveillance & Society 485 at 486.

[90] Colin Bennett, "In Further Defence of Privacy" (2011) 8:4 Surveillance & Society 513 at 514.

[91] Clarke, *supra* note 34; Finn et al, *supra* note 35 (both as cited in Wright & Raab, *supra* note 34).

[92] Clarke, *supra* note 34, as cited in Wright & Raab, *supra* note 34.

issues are not important and should not be addressed; rather, privacy-related issues should be considered alongside the broad range of societal impacts of workplace surveillance, including social (e.g., discriminatory functioning of surveillance technologies), political (e.g., impact on freedom of speech), and psychological (e.g., increased stress levels), among others.

It may seem as though we are suggesting that a legislative approach (i.e., Law 2.0) to workplace surveillance will be ineffective for the regulation of EMAs. This is not the case. Rather, we contend that in its *current form* Bill 88, while a relatively early step toward EMA regulation in Ontario, is not a sufficient supplement to existing, and outdated, regulatory solutions that govern contemporary realities of workplace surveillance.

5. CONCLUSION

Despite existing as an attempt to better inform Ontario workers about the digital monitoring practices of their employers, in its current form, Bill 88 is not a meaningful supplement to the existing regulatory patchwork that governs electronic monitoring in the workplace. With its objective of enhancing transparency, Bill 88 is expected to increase awareness of workplace surveillance amongst workers, reduce negative perceptions of EMAs, and begin building strong trust relations between employers and employees. However, the Bill does not provide workers with autonomy and control over whether, when, and how they are monitored by their employers. Nor does Bill 88 place transparency obligations on the marketing and sale of invasive surveillance mechanisms by vendors or restrictions on employers regarding the reasons for surveillance, the types of surveillance mechanisms used, the methods for storing data, and the purposes for which that data can be used. This overlooks the stubborn actuality that EMAs are invasive by design and can be harmful when used as intended, *as well as* the possibility that EMAs may invite misuse by employers outside of their intended purpose. The framing of workplace surveillance harms within Bill 88 as an *individual* privacy issue that is solved through a regulatory mechanism of increased transparency dismisses the multitude of impacts and societal effects of surveillance (e.g., social, political, psychological, economic, etc.) and ultimately streamlines regulatory responses toward surface-level privacy solutions that not only discount the numerous facets of privacy alone (e.g., privacy of communication, privacy of thoughts and feelings) but also the prospect of solutions that regulate the invasive harm-generating mechanisms themselves. Indeed, there is little that Bill 88 offers over and above the uneven (or non-existent) distribution of privacy protections through employment contracts and the general duty that managerial discretion be exercised in good faith. Overall, Bill 88 is a missed opportunity to revise and update the uneven patchwork quilt of regulation that touches on electronic monitoring in the workplace, and particularly those harms stemming from innovations in workplace surveillance technologies such as EMAs.

In light of the above concerns, we propose the following recommendations for the improvement of Bill 88. First, Bill 88 should move beyond its narrow conceptualization of workplace surveillance as an individual privacy issue to consider the broader dimensions of surveillance-related harms. This would allow for considerations of other societal impacts of workplace surveillance, including social (e.g., discriminatory effects of surveillance), political (e.g., impact on democratic rights such as free speech), and ethical (e.g., impacts on informed consent), psychological (e.g., impacts on job satisfaction and stress levels), among others. While these protections exist in various sections of the *Charter of Rights and Freedoms*, a more systematic legislative response that accounts for broader surveillance-related harms is warranted.

Second, Bill 88 should place restrictions on employers that clearly outline when surveillance can be justifiably used, the types of surveillance mechanisms that are permitted and prohibited, the purposes for which EMA data can be used, and how the data is to be stored by employers. Legislators may consider prohibiting the surveillance of employees outside of working hours (e.g., when on breaks), the use of invasive surveillance mechanisms (e.g., video surveillance, keystroke logging, and email or social media monitoring), and the use of EMA data for disciplinary purposes (e.g., to impair performance appraisals or thwart raise increases). Legislators should also outline procedures for the storage of EMA data that protect the privacy and anonymity of workers' data and prohibit the sharing of this information with third parties. To ensure the compliance of organizations with these regulations, legislators may consider requiring the submission of an annual report detailing the EMA software used, the purpose of surveillance, the surveillance mechanisms employed, and how the data was utilized. Audits may be conducted of organizations whose reports contain indications of non-compliance with the legislation.

And third, while we may not be able to give workers the right to entirely refuse employer surveillance, Bill 88 should be amended to give employees the right to file complaints to the Minister of Labour, Training and Skills Development related to the content of their company's monitoring policy or incidences of company non-compliance with the policy and have those complaints investigated by the Information and Privacy Commissioner of Ontario. This will allow workers to report instances of excessive and invasive forms of employer surveillance without having to resort to recourse through a costly and cumbersome tort of intrusion upon seclusion.

Bill 88 is an early and important step toward regulating workplace surveillance; however, a more comprehensive and systematic approach is necessary for governing electronic monitoring technologies. Provinces and territories that do not have an electronic monitoring law in place would benefit from the creation of legislation that incorporates the recommendations outlined within this article, but with the recommended amendments outlined above. By incorporating the above recommendations into Bill 88, governments can progress toward a comprehensive solution for the regulation of EMAs that

moves beyond individual privacy to protect workers from a broader panoply of surveillance-related harms.