The Telework Virus: How COVID-19 Has Affected Telework and Exposed Its Implications for Privacy

Tammy Katsabian†

The COVID-19 pandemic has shifted millions of people from working at their workplace to teleworking from home, generating a new normal: remote work. Remote work will be an integral part of the future of work and has positive implications for the employee, employer, and society. However, as this Article aims to demonstrate, remote work also involves problematic implications for workers' rights to privacy that arise from its hybrid, technology-based nature.

Remote work creates a new hybrid workspace for employees: the home-office. The home-office combines the logic and structure of the traditional workplace with those of the private sphere of the employee. As a result, the home-office creates an ongoing dilemma with respect to the privacy rights of the employee and anyone near her, especially her family. Because the work is conducted outside the physical workplace, employers are motivated to use various monitoring tools to ensure that the worker actually works. These programs give the employer a foothold in the private life of the employee that continually infringes on the privacy rights of the worker and her family. As this Article shows, this is possible because of the state of the law and the increasing evolution of dubious monitoring programs in the tech industry.

Against this background, this Article suggests ways to begin solving the privacy difficulty. Because of the hybrid nature of the home-office, the Article

DOI: https://doi.org/10.15779/Z38QF8JK7H

† Dr. Tammy Katsabian is an Associate Professor at The College of Management Academic Studies. This study was supported by the Fulbright Fund and the Emile Zola Chair for Interdisciplinary Human Rights. I would like to thank Matthew W. Finkin, Sunny Kalev, Guy Davidov, Guy Mundlak, Steve Bellovin, Einat Albin, Andrea Schneider, Gali Racabi, and Omer Kimhi for their careful reading and comments. I would also like to thank the organizers and participants in the "Northeast Privacy Scholars Workshop 13," the participants in the "Young Explorers Seminar YES," the participants in the Privacy Workshop at Tel Aviv University, the participants in the Tel Aviv University workshop on labor law, and the participant at the faculty of law workshop of the College of Management Academic Studies for their useful insights and comments. Lastly, I would like to thank the Berkeley Journal of Employment and Labor Law's editorial board for their thoroughly professional and excellent editing work. Any errors contained herein are mine.

argues that such solutions need to be applicable both in the workplace context and the tech industry. The Article then elaborates three leading principles to solve the privacy dilemma. The first is the proportionality approach. The current state of things leads to the "victory" of the employer's interests over the employee's right to privacy. The proportionality approach can rebalance this equation to ensure that the interests of both sides are considered. To ensure that such a balance is being achieved, the second principle is involving a representative of the employee in the process of evaluating the two parties' needs and rights such that they jointly generate a privacy policy tailored for that specific workplace. Finally, since monitoring companies are what enable the massive intrusion into the employee's private sphere, the last principle is incorporating privacy considerations throughout the process of engineering tracking programs, by following the privacy by design approach.

INTRODUCTION 143
I. THE HOME-OFFICE 147
A. Telework from Home Before COVID-19 148
B. Telework from Home During and After the COVID-19 Pandemic 149
II. THE HYBRID HOME-OFFICE AND ITS IMPLICATIONS FOR PRIVACY 154
A. Privacy in the Workplace Context 154
1. Monitoring Teleworkers in the Home-Office 157
2. The Right to Privacy 163
3. The Employer's Interests and Prerogatives 167
4. Between the Employee's Privacy and the Employer's Prerogatives 170
B. Third Parties as Privacy Violators 173
C. Third Parties as Victims: The "Side Effect" of Supervision of Teleworkers 174
III. THE QUESTION OF REGULATION 175
A. The Proportionality Approach 176
B. A Privacy Policy 180
C. The Privacy by Design Approach 185
IV. CONCLUSIONS 190

INTRODUCTION

Working from home ("teleworking") has become the new normal.[1] The COVID-19 pandemic forced numerous workers[2] to participate in the "largest global experiment in telecommuting in human history" and shift their working lives from the office to their private homes.[3] According to a Gallup study from October 2021, 45% of full-time employees are working partly or fully remotely, and nine in ten remote workers would like to continue working remotely to some degree.[4] A global work-from-home experience survey showed that approximately 25%–30% of the U.S. workforce will be working from home several days a week even after the pandemic is over.[5] Other research showed that in a post-pandemic world, an average person will

1. *See, e.g.*, INT'L LAB. ORG., COVID-19: GUIDANCE FOR LABOUR STATISTICS DATA COLLECTION 1 (June 5, 2020), https://www.ilo.org/wcmsp5/groups/public/—-dgreports/—-stat/documents/publication/wcms_747075.pdf [https://perma.cc/845C-QEBS] [hereinafter ILO TECHNICAL NOTE]; INT'L LAB. ORG., WORKING FROM HOME: ESTIMATING THE WORLDWIDE POTENTIAL (May 7, 2020), https://www.ilo.org/global/topics/non-standard-employment/publications/WCMS_743447/lang—en/index.htm [https://perma.cc/ERL5-4NPV] [hereinafter ILO POLICY BRIEF]; Erik Brynjolfsson et al., *COVID-19 and Remote Work: An Early Look at US Data* 1 (Nat'l Bureau of Econ. Rsch., Working Paper No. 27344, 2020), https://john-joseph-horton.com/papers/remote_work.pdf [https://perma.cc/MC6T-29RM]; Susan Hayter, *'Business as Unusual': How COVID-19 Brought Forward the Future of Work*, ILO BLOG: WORK IN PROGRESS (June 22, 2020), https://iloblog.org/2020/06/22/business-as-unusual-how-covid-19-brought-forward-the-future-of-work/#more-3367 [https://perma.cc/X7D9-R4W8]; Dominique Allen, *What If Flexibility Became the New Normal Post Covid-19?*, CANADIAN L. WORK F. (Apr. 23, 2020), http://lawofwork.ca/what-if-flexibility-became-the-new-normal-post-covid-19 [https://perma.cc/S5AV-JCUT]; Mackenzie Bouverat, *Today's News & Commentary*, ONLABOR (May 15, 2020), https://www.onlabor.org/todays-news-commentary-may-15-2020 [https://perma.cc/F33A-KP98]; *Office Re-Entry is Proving Trickier than Last Year's Abrupt Exit*, THE ECONOMIST (July 3, 2021), https://www.economist.com/business/2021/07/01/office-re-entry-is-proving-trickier-than-last-years-abrupt-exit [https://perma.cc/Y5GP-NBA5].

2. In the United States, there is no intermediate category between "employees" and "independent contractors." This Article refers to "workers" and "employees" interchangeably.

3. Dimitris Papanikolaou & Lawrence Schmidt, *Working Remotely and the Supply-Side Impact of COVID-19* 4 (Nat'l Bureau of Econ. Rsch., Working Paper No. 27330, 2020), https://www.nber.org/papers/w27330.pdf [https://perma.cc/F3EA-QDGS]. According to Gallup research, as of April 2020, approximately 62% of people in the American workforce have shifted to working from home due to COVID-19. Megan Brenan, *U.S. Workers Discovering Affinity for Remote Work*, GALLUP (Apr. 3, 2020), https://news.gallup.com/poll/306695/workers-discovering-affinity-remote-work.aspx [https://perma.cc/Y3XR-GRXJ]. According to another study that was based on a nationally representative sample of the U.S. population, as of the beginning of April 2020, approximately 34.1% of workers had switched to working from home. They joined 14.6% of workers who were already working from home. Brynjolfsson et al., *supra* note 1, at 3.

4. Lydia Saad & Ben Wigert, *Remote Work Persisting and Trending Permanent*, GALLUP (Oct. 13, 2021), https://news.gallup.com/poll/355907/remote-work-persisting-trending-permanent.aspx [https://perma.cc/GQL4-HDHM]. Another Gallup study showed that approximately 37% of offices will be empty in the future. Jim Clifton & Ben Wigert, *Bet on It: 37% of Desks Will Be Empty*, GALLUP (Dec. 7, 2021), https://www.gallup.com/workplace/357779/bet-desks-empty.aspx [https://perma.cc/8ZDH-44FT].

5. *Work-at-Home After Covid-19 – Our Forecast*, GLOB. WORKPLACE ANALYTICS, https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast [https://perma.cc/U9BT-CJD7].

work from home for at least 1.3 days a week.[6] Workers hope they will spend an even larger share—closer to half—of their working hours at the kitchen table.[7] A survey by Microsoft from March 2021 went even further, stressing that "the next great disruption is hybrid work."[8] A special report from the Organisation for Economic Co-operation and Development (OECD) similarly stressed that working from home is shifting from being a niche, temporary phenomenon to being a large share of the population's permanent way of working in today's world.[9] *MIT Technology Review*'s editors named remote work one of "ten breakthrough technologies for 2021."[10] Likewise, the *Guardian* announced on December 2021, "get used to it: working from home may be for life."[11] In other words, according to numerous forecasts, the move to remote work "has the potential to be the most transformative labour change in a generation,"[12] and this transformation is here to stay.

This massive shift to remote work is considered to have many benefits for society during the COVID-19 pandemic and beyond.[13] However, along with its advantages for employers and employees, especially during the COVID-19 crisis, working from home has problematic implications for workers.[14] As this Article intends to show, this is particularly true with regard to the right to privacy.

---

6. *Remote-first Work Is Taking over the Rich World*, THE ECONOMIST (Oct. 30, 2021), https://www.economist.com/finance-and-economics/2021/10/30/remote-first-work-is-taking-over-the-rich-world [https://perma.cc/R54B-XWY5].

7. *Id.*

8. The survey further emphasized that working from home is "here to stay." *See* THE NEXT GREAT DISRUPTION IS HYBRID WORK—ARE WE READY?, MICROSOFT (Mar. 2021), https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work [https://perma.cc/4V4Y-D6XQ].

9. OECD, EXPLORING POLICY OPTIONS ON TELEWORKING: STEERING LOCAL ECONOMIC AND EMPLOYMENT DEVELOPMENT IN THE TIME OF REMOTE WORK 7–8 (2020), https://doi.org/10.1787/5738b561-en [https://perma.cc/9BN2-BGW6] [hereinafter OECD 1]. A similar argument can be found in ILO TECHNICAL NOTE, *supra* note 1, at 3. Another study by the OECD from July 2021 tracks the exact numbers of teleworkers during COVID-19 all around the world. *See* OECD, MEASURING THE TELEWORK IN THE COVID-19 PANDEMIC (2021) https://www.oecd-ilibrary.org/docserver/0a76109f-en.pdf [https://perma.cc/PT5Z-6Z6H] [hereinafter OECD 2].

10. *10 Breakthrough Technologies 2021*, MIT TECH. REV. (Feb. 24, 2021), https://www.technologyreview.com/2021/02/24/1014369/10-breakthrough-technologies-2021 [https://perma.cc/JDM5-LQMC].

11. Imogen West-Knights, *Get Used to It: Working from Home May be for Life, Not Just for Christmas*, GUARDIAN (Dec. 13, 2021), https://www.theguardian.com/commentisfree/2021/dec/13/working-from-home-for-life-not-christmas-covid-england-rules [https://perma.cc/D3CZ-K3AS].

12. Phil Lord, *The Social Perils and Promise of Remote Work*, 4 J. BEHAV. ECON. FOR POL'Y 63, 63 (2020).

13. *See infra* notes 62–71 and accompanying text.

14. *See, e.g.*, Jodi Oakman et al., *A Rapid Review of Mental and Physical Health Effects of Working at Home: How Do We Optimise Health?*, 20 BMC PUB. HEALTH 1825 (2020); PROJECT INCLUDE, REMOTE WORK SINCE COVID-19 IS EXACERBATING HARM (Apr. 2021), https://projectinclude.org/assets/pdf/Project_Include_Harassment_Report_0321_R8.pdf

As demonstrated in this Article, this privacy issue is rooted in the fact that working from home generates a hybrid category, or sphere, in employment law: the "home-office." The home-office is an intermediate category between the office and the home that is possible because of widespread use of technology. The development of information communication technology (ICT) enables the typical office worker to easily and remotely connect to professional data and transform her home into her professional space.[15] In this reality, the home-office combines the logic and structure of the traditional office with that of the individual's private familial space. In doing so, the home-office embraces problematic aspects of the workplace, reproducing and strengthening them in the home context.

To be more precise, working from home involves methods of supervision more intrusive than those of the workplace, in which employees are casually observed by their managers or colleagues.[16] Since the beginning of the pandemic, numerous new monitoring features and programs have been developed and marketed widely. They take photographs and videos of the employee's screen and presence or constantly monitor whatever her activities at any given moment—all to ensure that she actually works from home.[17] Similarly, sometimes employers use tracking programs to ensure there are no cybersecurity risks when the employee works from home.[18] Using such

---

[https://perma.cc/3Q9C-EMDB]; FERNANDO G. BENAVIDESA ET AL., REVISTA BRASILEIRA DE SAÚDE OCUPACIONAL, THE FUTURE OF WORK AFTER THE COVID-19, THE UNCERTAIN ROLE OF TELEWORKING AT HOME (2021), https://www.scielo.br/j/rbso/a/LhzNSwFdfBKbwLQbv3Rntmt/?format=pdf&lang=en [https://perma.cc/ZS28-86GE] (discussing workers' health and well-being). *See, e.g.*, EUROFOUND, TELEWORKABILITY AND THE COVID-19 CRISIS: A NEW DIGITAL DIVIDE? 52–53 (2020), https://www.regionalstudies.org/wp-content/uploads/2020/08/Teleworkability-and-the-COVID-19-Crisis-A-New-Digital-Divide.pdf [https://perma.cc/WL9C-JEDZ] (discussing workers' sense of community). *See* Tammy Katsabian, *It's the End of Working Time as We Know It – New Challenges to the Concept of Working Time in the Digital Reality*, 65 MCGILL L.J. 379 (2020) (discussing workers' rights to genuine rest time). *See* Nicola Countouris & Valerio De Stefano, *The 'Long Covid' of Work Relations and the Future of Remote Work*, SOC. EUR. (Apr. 14, 2021), https://socialeurope.eu/the-long-covid-of-work-relations-and-the-future-of-remote-work [https://perma.cc/3UWD-QNXW] (discussing workers' basic classification as employees).

15. *See, e.g.*, TIM DWELLY, DISCONNECTED: SOCIAL HOUSING TENANTS AND THE HOME WORKING REVOLUTION 10 (2002); WORKING ANYTIME, ANYWHERE: THE EFFECTS ON THE WORLD OF WORK 1 (2017), http://www.ilo.org/wcmsp5/groups/public/—-dgreports/—-dcomm/—-publ/documents/publication/wcms_544138.pdf [https://perma.cc/984N-8TVZ]; W.C. Bunting, *Unlocking the Housing-Related Benefits of Telework: A Case for Government Intervention* 3–4 (Aug. 2, 2017); *see also* Kelly Garrett & James N. Danziger, *Which Telework, Defining and Testing a Taxonomy of Technology-Mediated Work at a Distance*, 25 SOC. SCI. COMPUT. REV. 27, 28 (2007); Tracey Crosbie & Jeanne Moore, *Work–Life Balance and Working from Home*, 3 SOC. POL'Y & SOC'Y 223, 224 (2004).

16. *See, e.g.*, Will Douglas Heaven, *This Startup Is Using AI to Give Workers a "Productivity Score"*, MIT TECH. REV. (June 4, 2020), https://www.technologyreview.com/2020/06/04/1002671/startup-ai-workers-productivity-score-bias-machine-learning-business-covid [https://perma.cc/K5AB-8TNF].

17. See *infra* Part II.A.1 for a detailed and comprehensive description of all these distance monitoring tools.

18. *See infra* notes 171–179 and accompanying text.

intrusive methods of supervising the employee seems even more offensive when they involve the employee's private computer or home.[19]

Additionally, in the home context, these monitoring programs may involve third parties as both the supervised and the privacy violators.[20] The employer, while supervising the employee at home, is capable of accessing personal data in the employee's virtual and real-world surroundings, including surveilling her private correspondence with friends and family members or surveilling her family members themselves, including minors. The ability to extensively supervise employees from home did not develop in a vacuum. It is possible because of the current state of the law, particularly the employer's legal prerogative to vet her employees when the information is considered relevant to the company's business needs. The tech industry massively developed monitoring programs in tandem with lenient state laws. These technologies might take random screenshots of the worker's computer, review video recordings of the worker's screen, install cameras in the worker's bedroom which couples as a workspace, or photograph the worker herself every ten minutes. As will be described throughout this Article, shifting to remote work[21] without considering the serious consequences that working from home has for the right to privacy and the various new entities that are influenced by it jeopardizes employees' and their family basic rights.

Against this background, this Article provides suggestions for addressing the challenges to privacy in remote work environments. The technological capacity for surveillance that employers have today favors the employer's profit interests over the privacy rights of the employee and their family. Following this reality, firstly I propose that the law should embrace a proportionality approach. Rather than prioritizing the employer's interests,

19. This is because the whole concept of privacy is based on the distinction between the employee's private sphere and her professional sphere. For further elaboration, see Tammy Katsabian, *Employees' Privacy in the Internet-Age – Towards a New Procedural Approach*, 40 BERKELEY J. EMP. & LAB. L. 203, 227–28 (2019).

20. *See, e.g.*, Ryan Fan, *Teachers, Do Not Use Zoom to Communicate with Students*, MEDIUM (Apr. 7, 2020), https://medium.com/@ryanfan/teachers-do-not-use-zoom-to-communicate-with-students-656634c14a1f [https://perma.cc/GQ4L-MLZ5].

21. Note that the shift to telework was encouraged also at the federal level well before the COVID-19 pandemic. *See* Telework Enhancement Act of 2010, 5 U.S.C. §§ 6501–6506; TELEWORK, https://www.telework.gov [https://perma.cc/6EBP-YXN4] (last visited Oct. 22, 2022). *See also* Jon C. Messenger, *Working Anytime, Anywhere: The Evolution of Telework and Its Effects on the World of Work*, IUSLABOR 303, 304–05 (Mar. 2017). Similar policies were developed during the pandemic in several states. *See* New York State Teleworking Expansion Act of 2020, 2021-2022 N.Y. Sess. Laws S. 5536 (referring to state employees in New York); Wes Venteicher, *As California Reopens, State Workers Urged Toward Telework*, GOV'T TECH. (June 5, 2020), https://www.govtech.com/workforce/As-California-Reopens-State-Workers-Urged-Toward-Telework.html [https://perma.cc/T3HG-7M4V] (referring mainly to state employees in California); COMMONWEALTH OF PA., OFF. OF THE GOVERNOR, ORDER OF THE GOVERNOR OF THE COMMONWEALTH OF PENNSYLVANIA FOR MITIGATION, ENFORCEMENT AND IMMUNITY PROTECTIONS (2020) (referring to all employees in Pennsylvania); *Telework Site*, PA. EMP. RES. CTR., https://www.oa.pa.gov/telework [https://perma.cc/DU5H-NH7U] (last visited Oct. 22, 2022) (referring to all state employees in Pennsylvania).

supervision of employees should be proportionate to all relevant circumstances, including the employee's right to privacy. To ensure a genuine proportional balance between employees' right to privacy and employers' business interests, employers should be obligated to negotiate a privacy policy regarding remote work with employees and their representatives. This sort of obligatory negotiating process would limit the employer's incursion into the employee's home-office and force employers to take employees' rights seriously. Additionally, due to the legal and technological sources of the privacy violation in the telework case, the strong link with the general surveillance culture, and the emergence of massive tracking programs for employers, companies that make tracking programs should also bear legal responsibilities. Specifically, they should be required to follow the "privacy by design" approach throughout the engineering and implementation of these monitoring programs.

To accomplish these aims, this Article proceeds as follows: Part I describes the home-office phenomenon and its different forms before and after the COVID-19 crisis. It focuses on the hybrid nature of the home-office and its roots in our contemporary digital reality. Part II focuses on the employee's right to privacy and the employer's interests in productivity and cybersecurity in the telework context. This Part explains how the home-office reproduces and exacerbates workplace privacy concerns in the employee's private sphere. It unpacks how the hybridity of the home-office infringes upon the employee's rights to privacy along with the right to privacy of third parties, such as family members, who lack any direct connection to the employee's workplace. In a parallel manner, Part II shows that tech companies are another crucial element of the home-office privacy challenge and discusses how these companies incentivize and normalize a problematic reality of employees teleworking. Part III then provides suggestions for regulating the home-office to address the privacy difficulty. It discusses the public-private sources of the home-office problem and offers solutions based on three guiding principles. It focuses on the model of proportionality, employees' representation in generating a privacy policy adapted to the workplace, and the privacy by design approach.

I. THE HOME-OFFICE

The phenomenon of working outside the office appeared well before the COVID-19 pandemic. There are different ways to conduct work away from the employer's premises.[22] One of the most common is described as

22. A special ILO report on this topic from June 2020 indicates that there are four main ways to conduct work away from the employer's premises. The first is remote work, which refers to "situations where the work is fully or partly carried out on an alternative worksite other than the default place of work." These sites are usually not the employee's home, but rather, for instance, the client's facilities or the public space. The second way is working at home, which takes place fully or partly within the

"telework"[23] (also known as "Information Communication Technology" or "ICT-mobile work,"[24] "remote work,"[25] and "work from home."[26]) Telework typically requires the employee to use a personal electronic device at an alternative location rather than the default place of work.[27] Accordingly, to "telework from home," the employee simply works at home with their personal electronic devices.[28] Telework can be full-time or part-time, meaning that people who only occasionally work outside the office on their electronic devices are also teleworkers.[29]

Telework is associated with ICT[30]—the technological infrastructure that enables the storage, use, transfer of, and access to, information on the internet.[31] ICT allows employees to easily receive information and transfer it to the workplace and to be available for work tasks outside the workplace anytime and from any place, all at a low financial cost.[32]

A. Telework from Home Before COVID-19

Telework, including telework from home, emerged in the U.S. labor market in the 1970s, when the information industry was developing.[33] A few decades later, when ICT became commonly available in every household through various daily-use devices such as laptops, tablets, and mobile phones, telework became more common worldwide.[34]

---

employee's residence. The third way is home-based work, which is a subcategory of the category of work at home. The fourth way is telework, on which this Article will be focused. *See* ILO TECHNICAL NOTE, *supra* note 1, at 5–7.

23. *See* the data *infra* regarding telework.

24. EUROFOUND & INT'L LAB. OFF., WORKING ANYTIME, ANYWHERE: THE EFFECTS ON THE WORLD OF WORK 1 (2017) http://www.ilo.org/wcmsp5/groups/public/—-dgreports/—-dcomm/—-publ/documents/publication/wcms_544138.pdf [https://perma.cc/984N-8TVZ].

25. Margrethe H. Olson, *Remote Office Work: Changing Work Patterns in Space and Time*, 26 COMMC'NS ACM 182, 182 (1983).

26. Audronė Nakrošienė, Ilona Bučiūnienė & Bernadeta Goštautaitė, *Working from Home: Characteristics and Outcomes of Telework*, 40 INT'L J. MANPOWER 87, 87 (2019).

27. ILO TECH. NOTE, *supra* note 1, at 6.

28. *Id.* at 7 (explaining the concept of "telework from home"). *See also* Brynjolfsson et al., *supra* note 1, at 3; Brenan, *supra* note 3.

29. EUROFOUND & INT'L LAB. OFF., *supra* note 24, at 5.

30. *See, e.g.*, DWELLY, *supra* note 15, at 10 (suggesting that ICT access is a key factor that allows households to engage in the benefits of telework).

31. James Murray, *Cloud Network Architecture and ICT: Modern Network Architecture* (Dec. 18, 2011), https://itknowledgeexchange.techtarget.com/modern-network-architecture/cloud-network-architecture-and-ict [https://perma.cc/55KW-JCJ4].

32. Freeman, *infra* note 64, at 288.

33. Jack M. Nilles, *Telecommunications and Organizational Decentralization*, 23 IEEE TRANSACTIONS ON COMMC'NS 1142 (1975); EUROFOUND & INT'L LAB. OFF., *supra* note 24, at 3, 11.

34. Jon C. Messenger & Lutz Gschwind, *Three Generations of Telework: New ICT and the (R)evolution from Home Office to Virtual Office*, 31 NEW TECH., WORK & EMP. 195, 196–97 (2016); EUROFOUND & INT'L LAB. OFF., *supra* note 24, at 3, 11; Jan Popma, *The Janus Face of the 'New Ways of Work': Rise, Risks and Regulation of Nomadic Work* (Eur. Trade Union Inst., Working Paper 2013.07,

In 2015, more than 50% of workplaces in the United States offered a position compatible with at least partial telework.[35] And in that year, 29% of all federal government employees occasionally conducted part of their work outside the office,[36] and 24% of all employed people performed some or all of their work at home.[37] By 2017, telework had become "a growing phenomenon, affecting up to one-third of employees in some . . . countries."[38] In 2017 to 2018, the share of employees who performed some or all of their work at home rose to 28.8%.[39] A more recent survey from 2019 found that 62% of respondents conducted telework.[40] Of those respondents, 30% were full-time teleworkers.[41]

Studies demonstrate similar realities in other countries.[42] An EU study from 2017 found that telework "varies substantially across countries, ranging between 2% and 40% of all employees, depending on the particular country and the frequency with which employees carry out T/ICTM work."[43] Finland, Japan, Sweden, and the Netherlands all have especially high rates of telework.[44] As will be shown in Part I.B, the COVID-19 pandemic is further increasing the number of full-time home teleworkers in the United States and around the world.

B. Telework from Home During and After the COVID-19 Pandemic

The COVID-19 crisis has highlighted the feasibility of telework from home, and it is becoming an integral and meaningful part of working life in

---

2013), https://www.etui.org/publications/working-papers/the-janus-face-of-the-new-ways-of-work-rise-risks-and-regulation-of-nomadic-work [https://perma.cc/9YRW-PUPE]; TIM DWELLY, DISCONNECTED: SOCIAL HOUSING TENANTS AND THE HOME WORKING REVOLUTION 4 (2002).

35. Kaytie Zimmerman, *Do Millennials Prefer Working from Home More Than Baby Boomers and Gen X?*, FORBES (Oct. 13, 2016), https://www.forbes.com/sites/kaytiezimmerman/2016/10/13/do-millennials-prefer-working-from-home-more-than-baby-boomers-and-gen-x/#3556a6754207 [https://perma.cc/TDB3-JFQE].

36. U.S. OFF. PERS. MGMT., FEDERAL EMPLOYEE VIEWPOINT SURVEY RESULTS: EMPLOYEES INFLUENCING CHANGE (2015), https://www.opm.gov/fevs/reports/data-reports/data-reports/report-by-agency/2015/2015-agency-report-part-1.pdf [https://perma.cc/5BC3-WR4P]; *see also* EUROFOUND & INT'L LAB. OFF., *supra* note 24, at 16.

37. *24 Percent of Employed People Did Some or All of Their Work at Home in 2015 on the Internet*, U.S. BUREAU OF LAB. STAT. (July 8, 2016), https://www.bls.gov/opub/ted/2016/24-percent-of-employed-people-did-some-or-all-of-their-work-at-home-in-2015.htm [https://perma.cc/7KXW-XUZL].

38. EUROFOUND & INT'L LAB. OFF., *supra* note 24, at 4.

39. *Economic News Release*, U.S. BUREAU OF LAB. STAT. (last modified Sept. 24, 2019), https://www.bls.gov/news.release/flex2.t01.htm [https://perma.cc/N34K-G5Z6].

40. OWL LABS, STATE OF REMOTE WORK 2019 (Sept. 2019), https://resources.owllabs.com/state-of-remote-work/2019 [https://perma.cc/Y3LD-8RP3].

41. *Id.*

42. *See New Forms of Employment*, EUROFOUND (Nov. 23, 2016), https://www.eurofound.europa.eu/new-forms-of-employment [https://perma.cc/SQ6G-2G4H] (presenting similar findings in other states).

43. Messenger, *supra* note 21, at 301.

44. *Id.* at 304–05.

the near future and perhaps the next big trend in the labor market.[45] Research from the beginning of the pandemic showed how the percentage of workers who telework from home rose in April 2020 to about 50%.[46] By that time, up to 62% of the U.S. workforce reported having worked remotely.[47] Other findings indicate a similar tendency, signaling a real transformation in the labor market even after the COVID-19 crisis is behind us.[48] According to a special global work-from-home experience survey, "those who were working remotely before the pandemic, will increase their frequency after they are allowed to return to their offices. For those who were new to remote work until the pandemic, we believe there will be a significant upswing in their adoption."[49] Another Gallup survey from May 2020 showed that half of the workers who were working from home during the pandemic would like to continue doing so after the pandemic is over.[50] Workers will consider this as

45. *See supra* notes 1–12 and accompanying text.

46. *See* Brynjolfsson et al., *supra* note 1, at 3.

47. *See* Brenan, *supra* note 3.

48. This is true for other countries in addition to the United States; according to research made by the Eurofound and the OECD, around 40% of Europe and OECD's population has shifted to full time telework at the beginning of the pandemic. OECD 1, *supra* note 9, at 8. *See also* Alexander Bick et al., *Work from Home After the COVID-19 Outbreak* 2 (Fed. Rsrv. Bank Dall., Working Paper No. 2017, July 2020), https://www.dallasfed.org/~/media/documents/research/papers/2020/wp2017r1.pdf [https://perma.cc/JEA2-BY87] (stating that "35.2 percent of workers [surveyed] worked entirely from home in May, compared to 8.2 percent in February"); OECD, OECD EMPLOYMENT OUTLOOK 2020: WORKER SECURITY AND THE COVID-19 CRISIS 12 (2020), https://doi.org/10.1787/1686c758-en [https://perma.cc/U3JJ-J2BG] [hereinafter OECD 3] (stating that "[a]n unprecedented number of workers (39% on average) shifted to telework" during the pandemic); Matthew Haag, *Manhattan Faces a Reckoning If Working from Home Becomes the Norm*, N.Y. TIMES (May 12, 2020), https://www.nytimes.com/2020/05/12/nyregion/coronavirus-work-from-home.html [https://perma.cc/BTF7-Y3ER] (demonstrating how, after COVID-19 lockdown, numerous leading companies in Manhattan were about to move to teleworking from home); Michael Maiello, *Only 37 Percent of US Jobs Can Be Done at Home*, CHI. BOOTH REV. (Apr. 24, 2020), https://review.chicagobooth.edu/economics/2020/article/only-37-percent-us-jobs-can-be-done-home [https://perma.cc/CF3F-7TZP] (referring to research showing that working from home will increase after the pandemic, but suggesting that there is an upper limit of 37% of jobs that can be conducted from home); Dylan Byers, *Mark Zuckerberg: Half of Facebook May Work Remotely by 2030*, NBC NEWS (May 21, 2020), https://www.nbcnews.com/tech/tech-news/mark-zuckerberg-half-facebook-may-work-remotely-2030-n1212081 [https://perma.cc/3K4H-L2SL] (citing Nicholas Bloom, a Stanford economics professor, who anticipates that the number of people who are working from home will double after the pandemic); Sarah Holder, *Paying Remote Workers to Relocate Gets a Pandemic-Era Boost*, BLOOMBERG (June 23, 2020), https://www.bloomberg.com/news/articles/2020-06-23/cities-are-looking-to-lure-newly-remote-workers [https://perma.cc/YD64-6JBF] (showing how the increase in teleworking from home leads to the side effect of relocation when people do not have to live near a physical workplace, further suggesting that teleworking from home is here to stay).

49. GLOB. WORKPLACE ANALYTICS, *supra* note 5.

50. Adam Hickman & Lydia Saad, *Reviewing Remote Work in the U.S. Under COVID-19*, GALLUP (May 22, 2020), https://news.gallup.com/poll/311375/reviewing-remote-work-covid.aspx [https://perma.cc/7DS2-YQNL]. This is follow-up research to the research introduced in Brenan, *supra* note 3. McKinsey made similar findings in this regard. *See Reimagining the Office and Work Life After COVID-19*, MCKINSEY & CO. (June 8, 2020), https://www.mckinsey.com/business-functions/organization/our-insights/reimagining-the-office-and-work-life-after-covid-19 [https://perma.cc/CUL4-QWRU] (referring to surveys showing that "80 percent of people questioned

a factor when applying for new positions.[51] Microsoft research from March 2021 similarly showed that 73% of workers surveyed want flexible remote work options to continue.[52] An OECD comparative report from July 2021 demonstrated that "both employees and employers would intend to make greater use of teleworking than before the pandemic."[53]

Similarly, companies that have shifted to telework from home during the pandemic are likely to embrace this method of work in the future.[54] This appears to be especially common among Big Tech companies, whose core work is based on computer networks.[55] Twitter announced that it will allow its employees to work from home "forever" if they wish to, even after the coronavirus pandemic has ended.[56] Facebook plans to shift approximately half of its workforce to working remotely over the next ten years.[57] Microsoft also plans to make a hybrid model of work possible for its employees even after the pandemic is over.[58] At Apple, workers challenged a new work arrangement that allowed them to work from home three days a week by

report that they enjoy working from home" and "forty-one percent say that they are more productive"). Finally, see in this context also OECD 1, *supra* note 9, at 8 (referring to surveys showing that "80% of American employees want to work from home at least some of the time, and over a third would take a pay cut in exchange for the option").

51. *See* OECD 1, *supra* note 9, at 8.

52. MICROSOFT, *supra* note 8, at 4.

53. OECD 2, *supra* note 9, at 4.

54. *See, e.g.*, Haag, *supra* note 48 ("Warren Buffett, the chairman of Berkshire Hathaway and one of the country's most prominent corporate leaders, predicted that the pandemic would lead many companies to embrace remote working arrangements."); *see also* Sophia Epstein, *They'd Rather Quit Than End the Remote Work Dream*, THE WIRED (Aug. 17, 2021), https://www.wired.co.uk/article/quit-remote-working-dream?mc_cid=77d2cd3ec9&mc_eid=d90a9de39d [https://perma.cc/DTB7-C83P] ("Not a day goes by without another company announcing a delay in its return to the office. Chevron, Facebook, McDonald's, even JP Morgan have all pushed back their plans to later this year or even 2022. But pressing pause may only postpone the fallout from employees who have grown used to the perks of remote work").

55. Rachel Lerman & Jay Greene, *Big Tech Was First to Send Workers Home. Now It's in No Rush to Bring Them Back*, WASH. POST (May 18, 2020), https://www.washingtonpost.com/technology/2020/05/18/facebook-google-work-from-home [https://perma.cc/P57T-GUX7] (noting that tech companies are "particularly well-suited" for remote work since many tasks "require computers and little else").

56. Dylan Byers, *Twitter Employees Can Work from Home Forever, CEO Says*, NBC NEWS (May 12, 2020), https://www.nbcnews.com/tech/tech-news/twitter-employees-can-work-home-forever-ceo-says-n1205346 [https://perma.cc/CC8W-W2U6]; Alex Kantrowitz, *Twitter Will Allow Employees to Work at Home Forever*, BUZZFEED NEWS (May 12, 2020), https://www.buzzfeednews.com/article/alexkantrowitz/twitter-will-allow-employees-to-work-at-home-forever [https://perma.cc/PK4W-XBPR].

57. Casey Newton, *Mark Zuckerberg on Taking His Massive Workforce Remote*, THE VERGE (May 21, 2020), https://www.theverge.com/2020/5/21/21265780/facebook-remote-work-mark-zuckerberg-interview-wfh [https://perma.cc/47H7-HY93] (quoting Facebook CEO Mark Zuckerberg as stating that "about half of the company" could be "working remotely permanently" within "10 years").

58. Tom Warren, *Microsoft to Start Reopening Headquarters on March 29th, with Hybrid Workplace Focus*, THE VERGE (Mar. 22, 2021), https://www.theverge.com/2021/3/22/22344273/microsoft-redmond-headquarters-open-hybrid-workplace [https://perma.cc/XV43-PYRJ]. See also Microsoft's survey on this matter finding that, for Microsoft employees, "[f]lexible work is here to stay." MICROSOFT, *supra* note 8, at 4.

demanding to *fully* telework from home, even after the pandemic is over.[59] In addition to these Big Tech companies, numerous other companies and governmental bodies around the world have announced their intention to shift to telecommuting.[60] For example, the United States Environmental Protection Agency will double the number of days allowed for telecommuting from two to four, which will enable its employees to keep working from home without the need to come into office at all.[61]

This massive shift to telework has many positive implications for the individual worker and employer, as well as for society as large. Remote work reduces traffic and air pollution.[62] It can also relieve some of the upward pressure on housing in metropolitan regions.[63] Remote work is cost effective for employers because it reduces the need for office space and transportation costs and increases productivity.[64] According to the OECD, employers can

59. Shirin Ghaffary & Rani Molla, *The Real Stakes of Apple's Battle over Remote Work*, VOX (Sept. 24, 2021), https://www.vox.com/recode/22690190/apple-remote-work-from-home-employee-cher-scarlett-janneke-parrish [https://perma.cc/5ANG-JKHV]. Apple delayed its return to office three months later, allowing its employees to continue to telework from home until further notice. Tim Higgins, *Apple Delays Return to Office, Closes Three Retail Stores as Covid Cases Rise*, WALL ST. J. (Dec. 15, 2021), https://www.wsj.com/articles/apple-delays-return-to-office-closes-three-retail-stores-as-covid-cases-rise-11639609890 [https://perma.cc/2QKE-V46Z].

60. For instance, Cerner and ViacomCBS announced that most, if not all, of their employees will continue working from home even after the pandemic is over. Tracy Platt, *The Future of Our Workplace: Flexibility to Manage Work and Life at Cerner*, ORACLE CERNER (June 3, 2021), https://www.cerner.com/newsroom/the-future-of-our-workplace-at-cerner [https://perma.cc/ZKP2-FYQA]; Elaine Low, *ViacomCBS Unveils Post-COVID Work Model: 70% of Staff to Split Time Between Home and Office*, VARIETY (Nov. 19, 2020), https://variety.com/2020/tv/news/viacomcbs-unveils-post-covid-work-model-70-of-staff-to-split-time-between-home-and-office-exclusive-1234836161 [https://perma.cc/9QV6-MFN2]. Unum went further and announced that roughly 400 employees who worked from Unum's downtown Massachusetts office will now work from home permanently and the office location will be closed. Steven H. Foskett, *Unum Closing Worcester Office, 400 Employees to Work at Home*, TELEGRAM & GAZETTE (July 16, 2020), https://www.telegram.com/news/20200716/unum-closing-worcester-office-400-employees-to-work-at-home [https://perma.cc/6YD7-8VSE]. Finally, close to a fifth of surveyed companies in San Francisco Bay Area businesses predicted that they would likely transition to full telework after the pandemic has diminished. *New CEO Survey Finds Dramatic Workplace Changes in Response to COVID-19*, BAY AREA COUNCIL (May 15, 2020), https://www.bayareacouncil.org/press-releases/new-ceo-survey-finds-dramatic-workplace-changes-in-response-to-covid-19 [https://perma.cc/7HPS-LX3R].

61. William Greenlaw, *Today's News & Commentary*, ONLABOR (Dec. 2, 2021), https://onlabor.org/todays-news-commentary-december-2-2021 [https://perma.cc/L9W5-PRDJ].

62. Eleftherios Giovanis, *The Relationship Between Teleworking, Traffic and Air Pollution*, 9 ATMOSPHERIC POLLUTION RSCH. 1, 12 (2018); CITI GPS, TECHNOLOGY AT WORK V5.0: A NEW WORLD OF REMOTE WORK 98–104 (2020), https://www.oxfordmartin.ox.ac.uk/downloads/reports/CitiGPS_TechnologyatWork_5_220620.pdf.

63. Jerusalem Demsas, *3 Ways Remote Work Could Remake America*, VOX (Jan. 4, 2022), https://www.vox.com/22839563/remote-work-climate-change-house-prices-cities [https://perma.cc/QB38-UPN8] (referring also to the positive implications of remote work for climate change and politics).

64. Stephen Ruth & Imran Chaudhry, *Telework: A Productivity Paradox?*, 12 IEEE INTERNET COMPUTING 87, 87 (2008); Richard B. Freeman, *The Labour Market in the New Information Economy*, 18 OXFORD REV. ECON. POL'Y 288, 295 (2002); Courtney Rubin, *The Office Is Dead*, MARKER (May 11, 2020), https://marker.medium.com/the-office-is-dead-16be89f25d01 [https://perma.cc/7678-BXRX].

save approximately $11,000 per year for every worker working remotely half of the time.[65] Further, remote work during the pandemic enables employers to keep doing ongoing work without exposing their employees to unnecessary risks and without offices adjusting to new restrictions and public health rules.[66] Finally, remote work has positive implications for employees as well because of preferable schedules and better work-life balance.[67] Many employees choose to work from home because it provides more flexibility and allows them to enjoy a less stressful work environment.[68] Parents in particular prefer to work from home for better work-life balance.[69] Working from home during the COVID-19 pandemic has been particularly beneficial to employees because they can keep their jobs, maintain their income,[70] and work in a safe place without being exposed to colleagues or clients who might be infected with the virus.[71]

However, as the following parts will show, the eagerness of all parties to continue the trend of teleworking, at least partly, and the benefits telework has for all also comes with problematic and far-reaching side effects for workers' privacy. Part II focuses on this question.

65. OECD 1, *supra* note 9, at 9; *see also* GLOB. WORKPLACE ANALYTICS, *supra* note 5 (explaining that working from home reduces wasted office costs because employees do not spend much time at their workplace desks).

66. Papanikolaou & Schmidt, *supra* note 3, at 4–6; Sarah H. Bana et al., *Ranking How National Economies Adapt to Remote Work*, MIT SLOAN MGMT. REV. (June 18, 2020), https://sloanreview.mit.edu/article/ranking-how-national-economies-adapt-to-remote-work [https://perma.cc/7LCY-GQZG].

67. Phyllis Moen et al., *Does a Flexibility/Support Organizational Initiative Improve High-Tech Employees' Well-Being?*, 81 AM. SOCIO. REV. 134, 155–58 (2016). *See also* Lonnie Golden & Jaeseung Kim, *Irregular Work Scheduling and Its Consequences*, *in* WORK–LIFE BALANCE IN THE MODERN WORKPLACE 129–30 (Sarah De Groof ed., 2017) (describing an Obama directive to initiate more flexible workplace options for federal employees, with telework as one suggestion).

68. MELISSA GREGG, WORK'S INTIMACY 39–40 (1st ed. 2011).

69. Emilie Genin, *The Third Shift: How Do Professional Women Articulate Working Time and Family Time?*, *in* WORK-LIFE BALANCE IN THE MODERN WORKPLACE 103, 108–09 (Sarah De Groof ed., 2017).

70. *See* Papanikolaou & Schmidt, *supra* note 3, at 13–14 (showing how COVID-19 has mainly harmed workers who could have work remotely rather than workers who could easily telecommute); *see also* CITI GPS, *supra* note 62, at 48. See also the OECD findings that "the OECD-wide unemployment rate rose from 5.3% in January to 8.4% in May." OECD 3, *supra* note 48, at 12.

71. CITI GPS, s*upra* note 62, at 48. This is unlike workers in other positions who were forced to come to the workplace and exposed to the danger of becoming infected by the coronavirus. *See, e.g.*, Ezra Kaplan & Jo Ling Kent, *Eighth Amazon Warehouse Worker Dies from COVID-19*, CBS NEWS (May 22, 2020), https://www.nbcnews.com/news/us-news/eighth-amazon-warehouse-worker-dies-covid-19-n1212546 [https://perma.cc/UB44-TMNA]; Monica Nickelsburg, *Warehouse Workers Sue Amazon over COVID-19 Exposure After Death of an Employee's Relative*, GEEKWIRE (June 4, 2020), https://www.geekwire.com/2020/warehouse-workers-sue-amazon-covid-19-exposure-death-employees-relative [https://perma.cc/H963-7ANM].

II. THE HYBRID HOME-OFFICE AND ITS IMPLICATIONS FOR PRIVACY

The growing phenomenon of teleworking from home, as discussed above, provides various benefits for the individual and the society, but it also generates a hybrid space in the future workplace. This hybrid space is metaphorically located somewhere between the home and the office: the home-office. The home-office is a hybrid location because it combines two human spheres, the private and the professional, encapsulating the both the private life and professional life of the worker. Specifically, the home-office includes actors and relationships that are both private and professional—it incorporates the worker's family members along with her colleagues, clients, managers, and supervisors. Further, the home-office combines work tasks with the worker's ordinary familial routine, continually blurring the border between working time and private rest time.[72]

As I will argue, the home-office's hybrid nature magnifies and reproduces problematic aspects of the workplace in the home and, in doing so, increases the potential for violation of the employee's right to privacy. As Part II.A will show, this trend is particularly problematic when viewed against the backdrop of the pandemic and the expanding surveillance culture enabled by growing technological capabilities of employers to supervise their employees anytime and anywhere.

A. Privacy in the Workplace Context

Surveillance of workers has become a common phenomenon in today's world. It includes "management's ability to monitor, record and track employee performance, behaviors and personal characteristics in real time . . . or as part of broader organizational processes."[73]

To be sure, employers have always wanted to increase their surveillance of workers and acquire knowledge about their workers outside the workplace.[74] Digital reality and its numerous surveillance technologies have dramatically increased employers' ability to probe their employees' private lives.[75] Today, employers can easily supervise and monitor their employees

72. *See generally* Katsabian, *supra* note 14.

73. Kirstie Ball, *Workplace Surveillance: An Overview*, 51 LAB. HIST. 87, 87 (2010).

74. KARL MARX, I CAPITAL chs. 10, 13–15, 17, 25 (1867); Checking on Ford Employees Home Conditions, Views from "Factory Facts from Ford," 1917 (photograph), HENRY FORD, https://www.thehenryford.org/collections-and-research/digital-collections/artifact/109833 [https://perma.cc/YWU7-TBFJ] (last visited Oct. 22, 2022).

75. DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 22-34 (1994); Ifeoma Ajunwa et al., *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735, 737–40 (2017); Kim T. Pauline, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 860–61 (2017); Priscilla M. Regan, *Genetic Testing and Workplace Surveillance: Implications for Privacy*, *in* COMPUTERS, SURVEILLANCE, AND PRIVACY 21, 21–23 (David Lyon & Elia Zureik eds., 1996); Janis L. Goldie, *Virtual Communities and the Social Dimension of Privacy*, 3 OTTAWA LAW & TECH. J. 133, 142 (2006); Yanisky-Ravid, *infra* note 156, at 63–71.

beyond the conventional boundaries of the workplace.[76] Technology has made the entire process of supervising easier to manage. It has enabled the employer to supervise an employee even without the employee's awareness,[77] often at a relatively low cost.[78] This is particularly true in the era of artificial intelligence (AI) technologies, which enable employers to easily process vast amounts of information on an employee, even private information, secretly.[79] AI has enabled the employer to easily view, collect, process, analyze, and preserve professional and private information on the employee, from when they were merely a candidate for employment and to even after they leave the employer.[80] As a result, the average workplace in today's world is inundated with more information on its employees than ever before.[81]

The surveillance culture—i.e., the banal phenomenon of being watched by the state as part of the capitalist model in the digital reality—has further augmented the impact of technological possibilities and the desire of employers to constantly vet their employees.[82] The COVID-19 pandemic has strengthened the casualness of the surveillance culture, leading to even more supervision of the individual in her private sphere.[83] As an example, to help

76. Ajunwa et al., *supra* note 75, at 737–41.

77. Goldie, *supra* note 75, at 142–45; Sue Shellenbarger, *Work at Home? Your Employer May Be Watching*, WALL ST. J. (July 30, 2008), https://www.wsj.com/articles/SB121737022605394845 [https://perma.cc/BT4C-H8DY].

78. LAWRENCE LESSIG, CODE: VERSION 2.0 200 (2d ed. 2006) (explaining that the Internet has produced a "lack of control" over our private data due to "perpetual and cheap monitoring of behavior").

79. Matthew T. Bodie et al., *The Law and Policy of People Analytics*, 88 U. COLO. L. REV. 961, 1005–06, 1019 (2016); Valerio De Stefano, *"Negotiating the Algorithm": Automation, Artificial Intelligence, and Labor Protection*, 41 COMP. LAB. L. & POL'Y J. 15, 15–16 (2019); Solon Barocas & Andrew Selbst, *Big Data's Disparate-Impact*, 104 CALIF. L. REV. 671 (2016); Brishen Rogers, *The Law and Political Economy of Workplace Technological Change*, 55 HARV. C.R.-C.L. L. REV. 531 (2020); Arianne Renan Barzilay, *Data Analytics at Work: A View from Israel on Employee Privacy and Equality in the Age of Data-Driven Employment Management*, 40 COMP. LAB. L. & POL'Y J. 421, 422–26 (2019); Jeffrey M. Hirsch, *Future Work*, 2020 U. ILL. L. REV. 889 (2020).

80. Bodie et al., *supra* note 79, at 973–78, 1014–18.

81. *See* Ajunwa et al., *supra* note 75, at 763–72.

82. *See generally* David Lyon, *Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity*, 11 INT'L J. COMMC'N 824 (2017) (elaborating on the phenomenon of surveillance culture in the digital reality); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019) (describing the phenomenon of surveillance culture as part of the modern capitalist model).

83. Andrew Roth et al., *Growth in Surveillance May Be Hard to Scale Back After Pandemic, Experts Say*, GUARDIAN (Apr. 14, 2020), https://www.theguardian.com/world/2020/apr/14/growth-in-surveillance-may-be-hard-to-scale-back-after-coronavirus-pandemic-experts-say [https://perma.cc/9V58-H32L]; Yossi David & Elisabeth Sommerlad, *Media and Information in Times of Crisis: The Case of the COVID-19 Infodemic*, *in* COVID-19 AND SIMILAR FUTURES: PANDEMIC GEOGRAPHIES (Andrews et al. eds., forthcoming); Michele L. Norris, *Opinion: Thanks to Covid-19, the Age of Biometric Surveillance Is Here*, WASH. POST (Mar. 22, 2021), https://www.washingtonpost.com/opinions/thanks-to-covid-19-the-age-of-biometric-surveillance-is-here/2021/03/22/04b24f76-8b24-11eb-a6bd-0eb91c03305a_story.html [https://perma.cc/KF36-2FTF].

keep COVID-19 from spreading—by verifying, for instance, that people are social distancing,[84] staying at home while they are sick,[85] or by notifying someone that she was exposed to an infected person[86]—various states around the world have resorted to sophisticated tracking technologies.[87] Numerous reporters and scholars have warned about the vast destructive implications this phenomenon has for the right to privacy in the long run.[88]

The COVID-19 surveillance culture has also intruded into the workplace and affected employees' right to privacy. Employers are increasingly using tracking technologies in the physical workplace to ensure that workers are healthy when they enter or that they employ social distancing.[89] The ease with which employees are being supervised in the digital reality has

84. Tony Romm et al., *U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus*, WASH. POST (Mar. 18, 2020), https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus [https://perma.cc/5FNG-M9CA].

85. Raphael Satter, *To Keep COVID-19 Patients Home, Some U.S. States Weigh House Arrest Tech*, REUTERS (May 7, 2020), https://www.reuters.com/article/us-health-coronavirus-quarantine-tech/to-keep-covid-19-patients-home-some-u-s-states-weigh-house-arrest-tech-idUSKBN22J1U8 [https://perma.cc/MG8B-HZHU].

86. Will Douglas, *A New App Would Say If You've Crossed Paths with Someone Who Is Infected*, MIT TECH. REV. (Mar. 17, 2020), https://www.technologyreview.com/2020/03/17/905257/coronavirus-infection-tests-app-pandemic-location-privacy [https://perma.cc/DB6V-62EJ].

87. Dave Gershgorn, *We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World*, ONEZERO (Apr. 9, 2020), https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9 [https://perma.cc/PT24-EVHG]; Carolyn Schmitt, *Global Perspectives on Data Collection, Contact Tracing, and COVID-19*, BERKMAN KLEIN CTR. (Apr. 28, 2020), https://medium.com/berkman-klein-center/global-perspectives-on-data-collection-contact-tracing-and-covid-19-8fbbcfdff25f [https://perma.cc/362L-JZLE].

88. *See, e.g.*, Lorna McGregor, *Contact-tracing Apps and Human Rights*, EJIL:TALK! (Apr. 30, 2020), https://www.ejiltalk.org/contact-tracing-apps-and-human-rights [https://perma.cc/M3CL-PWQC]; Roth et al., *supra* note 83; Albert Fox Cahn & John Veiszlemlein, *COVID-19 Tracking Data and Surveillance Risks Are More Dangerous Than Their Rewards*, THINK (Mar. 19, 2020), https://www.nbcnews.com/think/opinion/covid-19-tracking-data-surveillance-risks-are-more-dangerous-their-ncna1164281 [https://perma.cc/KN8T-HGXA]; Benjamin Powers, *Privacy Advocates Are Sounding Alarms over Coronavirus Surveillance*, COINDESK (Mar. 23, 2020), https://www.coindesk.com/privacy-advocates-are-sounding-alarms-over-coronavirus-surveillance [https://perma.cc/K8YH-8PWZ].

89. *See generally* Matthew T. Bodie & Michael McMahon, *Employee Testing, Tracing, and Disclosure as a Response to the Coronavirus Pandemic*, 64 WASH. U. J. L. & POL'Y 31 (2020); Antonio Aloisi & Valerio De Stefano, *Essential Jobs, Remote Work and Digital Surveillance: Addressing the COVID-19 Pandemic Panopticon*, 161 INT'L LAB. REV. 289 (2022); Karen Hao, *Machine Learning Could Check if You're Social Distancing Properly at Work*, MIT TECH. REV. (Apr. 17, 2020), https://www.technologyreview.com/2020/04/17/1000092/ai-machine-learning-watches-social-distancing-at-work [https://perma.cc/MXN4-2YZP]; Natalie Chyi, *The Workplace-Surveillance Technology Boom*, SLATE (May 12, 2020), https://slate.com/technology/2020/05/workplace-surveillance-apps-coronavirus.html [https://perma.cc/BLY5-KAK5] (discussing in depth the various available programs in this regard and their use by well-known companies such as Amazon, Walmart, Johns Hopkins Hospital, and Mayo Clinic).

generated a concerning tolerance of other forms of privacy violation.[90] It has essentially made employee privacy violations more acceptable.

1. Monitoring Teleworkers in the Home-Office

One of the most distinctive examples of this occurs in the case of the home-office. The COVID-19 pandemic has not only shifted people to teleworking from home, it has also enabled an excessive degree of surveillance of teleworkers' activities at home.[91] Employees working in home-offices rather than the traditional workplace has motivated employers to surveil worker productivity.[92] This is because in the workplace, employees can be casually observed by their managers or colleagues since they are all part of the same physical space. By contrast, when it comes to remote work, employers feel that they must use additional methods to ensure that their workers are actually working from home and not spending their working day on personal activities. Following this tendency, the degree and intensity of monitoring of workers' activities throughout the workday are increasing.[93] According to an NBC News article from August 2021, Big Tech call center teleworkers face pressure to accept home surveillance that includes "monitoring by AI-powered cameras in workers' homes, voice analytics and storage of data collected from the worker's family members, including minors."[94] Indicative of this is that since the beginning of the COVID-19 pandemic in the United States, sales of various surveillance apps that

90. *See* Chyi, *supra* note 89; Aiha Nguyen, *On the Clock and at Home: Post-COVID-19 Employee Monitoring in the Workplace*, PEOPLE + STRATEGY J. (Summer 2020), https://www.shrm.org/executive/resources/people-strategy-journal/summer2020/pages/feature-nguyen.aspx [https://perma.cc/W3JE-Z8AW].

91. *See, e.g.*, Heaven, *supra* note 16; Bobby Allyn, *Your Boss Is Watching You: Work-from-Home Boom Leads to More Surveillance*, NPR (May 13, 2020), https://www.npr.org/2020/05/13/854014403/your-boss-is-watching-you-work-from-home-boom-leads-to-more-surveillance [https://perma.cc/D99Y-B8XM]; Barclay Ballard, *One in Five Firms Admit to Illegally Spying on Employees Working from Home*, TECHRADAR (Jan. 19, 2021) https://www.techradar.com/news/one-in-five-firms-admit-to-illegally-spying-on-employees-working-from-home [https://perma.cc/79S9-TTUR].

92. *See* Susan Bryant, *Electronic Surveillance in the Workplace*, 20 CANADIAN J. COMMC'N 505 (Apr. 1995), https://doi.org/10.22230/cjc.1995v20n4a893 [https://perma.cc/73LX-KBRL] ("for all telecommuters, unionized or not, there is an increased potential for electronic surveillance to be rationalized by employers—'since we can't see you, it only makes sense that we must supervise you electronically' might be the argument made"); Amy Vatcha, *Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees*, 15 IS CHANNEL 4, 4 (2020) ("[I]n the era of technology, flexible working, and fluid boundaries between the home and office, workplace monitoring for business reasons often extends into one's personal life leading to all round employee monitoring.").

93. *See* works cited *supra* note 91; *supra* note 92.

94. Olivia Solon, *Big Tech Call Center Workers Face Pressure to Accept Home Surveillance*, NBC NEWS (Aug. 8, 2021), https://www.nbcnews.com/tech/tech-news/big-tech-call-center-workers-face-pressure-accept-home-surveillance-n1276227 [https://perma.cc/X7UY-H72V].

supervise workers' activity from a distance have dramatically increased.[95] Similarly, more and more firms have admitted that they began to use remote tracking technology to track and monitor their employees' productivity.[96]

In this way, numerous tracking programs have become widely available since March 2020. Hubstaff software is such a program. It includes time tracking, GPS and location tracking, and productivity monitoring of the teleworker's activity.[97] This software is installed on the worker's computer, typically by the worker herself at the request of the employer.[98] It constantly records the worker's keyboard strokes, mouse movements, and websites visited, ensuring that workers devote all their time to work activities.[99] The software also takes random screenshots on the worker's computer.[100] By doing so, it seemingly enables employers to verify that their workers are indeed working. However, it also creates a concerning constant surveillance of the employee.

We can learn about this reality from the experience of Adam Satariano, a British reporter who volunteered to install Hubstaff software on his private computer and let his employer supervise his activities via the program.[101] In an article that was published in the *New York Times*, Satariano powerfully described the intensity of the supervision process he underwent. In this article, he emphasized the ease with which the software could access his private life, either when he conducted an online private activity during his work hours or, worse, when he conducted the activity during his leisure time

95. Samara Lynn, *As Employee Monitoring Extends to Workers' Homes and Health, Some See Civil Rights Threat*, ABC NEWS (May 23, 2020), https://abcnews.go.com/U9S/employee-monitoring-extends-workers-homes-health-civil-rights/story?id=70665085 [https://perma.cc/8TDN-BVXC] ("[T]here is evidence that monitoring software is seeing unprecedented adoption rates since the onset of COVID-19."); Adam Satariano, *How My Boss Monitors Me While I Work from Home*, N.Y. TIMES (May 6, 2020), https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html [https://perma.cc/QS7R-P84Z] (describing how the Hubstaff surveillance software (see below) tripled its sales between March 2020 and May 6, 2020); Drew Harwell, *Managers Turn to Surveillance Software, Always-On Webcams to Ensure Employees Are (Really) Working from Home*, WASH. POST (Apr. 30, 2020), https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance [https://perma.cc/6PP2-QWMV] (stating that "Pragli [a remote-tracking program] co-founder Vivek Nair . . . said user activity has 'exploded 20 times over since February'"). *See also* Polly Mosendz & Anders Melin, *Spy Software to Keep Tabs on Remote Workers*, BLOOMBERG (Mar. 27, 2020), https://www.bloomberg.com/news/features/2020-03-27/bosses-panic-buy-spy-software-to-keep-tabs-on-remote-workers [https://perma.cc/V9TN-HJ73] (citing statements of CEOs and spokespersons of tracking apps companies in this regard).

96. As an instance, according to a U.K survey from November 2020, 12% of all firms have already implemented tracking software in the U.K. Vivek Dodd, *Remote-working Compliance YouGov Survey*, SKILLCAST (Nov. 25, 2020), https://www.skillcast.com/blog/remote-working-compliance-survey-key-findings [https://perma.cc/45LT-QM5P].

97. HUBSTAFF, https://hubstaff.com [https://perma.cc/738V-SCFY] (last visited Sept. 16, 2022).

98. *See* Allyn, *supra* note 91; *see also* Heaven, *supra* note 16 (describing Hubstaff software); Mosendz & Melin, *supra* note 95 (further describing Hubstaff software).

99. *See* Heaven, *supra* note 16.

100. Satariano, *supra* note 95.

101. *Id.*

after forgetting to log out of the program.[102] The following testimony of Satariano exemplifies these points well:

> The moment when I no longer wanted to be monitored came on April 23 at 11:30 a.m., when Hubstaff caught me doing an internet exercise class. By the time I realized I had not logged out, it had snapped a screenshot of the trainer setting up to teach the class in her living room . . . What if other screenshots exposed sensitive health or financial information? I trust Pui-Wing [Satariano's supervisor] but the monitoring systems have few safeguards to prevent abuse, and they rely on managers exercising judgment and restraint.[103]

Like the Hubstaff software, other tracking programs have become very popular during the pandemic.[104] Another commonly used surveillance program is Time Doctor.[105] Time Doctor goes even further than the Hubstaff software by video recording the worker's screen or photographing the worker herself every ten minutes.[106] In this way, the program verifies that the worker is working in front of the computer during *all* her working time and deters her from leaving her seat even for a small break to stretch or even go to the bathroom. Another common surveillance program, Teramind, can be installed on a teleworker's devices, sometimes even without her knowledge.[107] This program enables the employer to monitor emails, applications, instant messages, keystrokes, social media usage, and any other activity on the computer.[108]

A fourth interactive monitoring system, Pragli (also known as 'Pesto'), creates avatars for each worker in a way that enables the workers to virtually communicate with one another.[109] In addition to measuring employees' keyboard and mouse usage to assess whether they are actively working, the Pragli system allows any worker to instantly start a video conversation with a colleague by clicking on the colleague's avatar. For this reason, the Pragli system encourages workers to always keep their home webcams and microphones on—at the expense of the workers' right to privacy—so "a spontaneous face-to-face chat [is] always only a click away."[110] Other

---

102. *Id.*

103. *Id.*

104. *See, e.g.*, ACTIVTRAK, https://www.activtrak.com [https://perma.cc/JHV6-7396] (last visited Sept. 16, 2022).

105. TIME DOCTOR, https://www.timedoctor.com [https://perma.cc/5N4C-UN53] (last visited Sept. 16, 2022).

106. Heaven, *supra* note 16 (describing the Time Doctor program); Allyn, *supra* note 91.

107. Lynn, *supra* note 95.

108. *Id.*; TERAMIND, *How Can I Monitor Employees' Computer Activity?* (May 28, 2021, 10:42 PM), https://kb.teramind.co/hc/en-us/articles/1500009065102-How-can-I-monitor-employees-computer-activity- [https://perma.cc/72CC-5QCL]. *See also* TERAMIND, https://www.teramind.co [https://perma.cc/TCR3-9YZ7] (last visited Oct. 22, 2022).

109. Harwell, *supra* note 95.

110. *Id.*

common tracking apps are installed on the employee's mobile phone which is often their personal phone. These apps keep tabs on the employee's whereabouts during work hours.[111] Again, the goal of these apps is to ensure that teleworkers devote all their working time to work activities.[112]

Alongside these apps, some employers also require their workers to install video cameras in the workers' working space to ensure that the worker actually works, even if employees worked from their bedrooms.[113] For example, Teleperformance's workers in Colombia and Albania testified how their employers sent them an eight-page addendum to their existing employment contracts that included a requirement to agree to new home surveillance rules.[114] According to a news report on this issue, as part of this new addendum, the employees were asked to:

> . . . . agree to having video cameras installed in their home or on their computers, pointing at their workspace, to record and monitor workers in real time. It also states that workers agree to Teleperformance using AI-powered video analysis tools that can identify objects around the workspace, including mobile phones, paper and other items that are restricted by Teleperformance's security policies. They must also agree to sharing data and images related to any children they have under the age of 18—who might get picked up by video and audio monitoring tools—and to sharing biometric data including fingerprints and photos.[115]

In addition to these monitoring programs and video cameras, there are other more sophisticated programs that not only supervise the teleworker's activity from a distance but also score the worker based on her online behavior. One example is software that runs in the background of the worker's computer (that is, usually, her personal computer when she works from home) and monitors *all* relevant activity and data during work time. Based on this data, an algorithm learns the worker's typical pattern of behavior, compares it to other workers' patterns, and gives each worker a "productivity score."[116] A similar AI program monitors interactions between teleworkers and examines the intensity of their work collaboration from home. Based on this information, along with the personal file of each worker, the program aims to identify and rate the most successful workers in the company.[117] Another program, which is based on machine-learning software, aims to measure how fast a worker accomplishes various work tasks and

111. Allyn, *supra* note 91; *see also* Ajunwa et al., *supra* note 75, at 743.

112. Allyn, *supra* note 91.

113. *Id.*

114. Solon, *supra* note 94.

115. *Id.*

116. Heaven, *supra* note 16 (describing "Enaible's software, which it calls the AI Productivity Platform").

117. *Id.* (referring to the Isaak program).

assigns a score. This program also offers the employer methods to speed up the worker's activity.[118]

Finally, the InterGuard program, which can be *secretly* installed on workers' computers, creates a minute-by-minute timeline of every app and website the worker views, categorizes each one of them as "productive" or "unproductive," and on this basis ranks workers with a "productivity score."[119] This system also records all emails, messages, and keystrokes and takes pictures of employees' screens every five seconds, which managers can review when they wish.[120]

Along with all these explicit remote tracking programs, there are many other seemingly innocuous remote work programs. One example for such a program is Microsoft 365, which "aggregate[s] all sorts of data into simple charts or graphs that give managers high-level view of what workers are doing."[121] Another example of a supposedly innocuous monitoring tool is the diverse new videoconferencing programs teleworkers use today.[122] The most well-known example is the Zoom platform.[123] As a consequence of the COVID-19 crisis and the shift to constantly being indoors, the number of daily average users of Zoom increased from around 10 million in December 2019 to around 200 million in March 2020[124] and 300 million in April 2020.[125] Zoom can be very beneficial for teleworkers, especially during the pandemic when it is not possible to go to the office.[126] However, Zoom is

118. *Id.* (referring to a new program in development).

119. Harwell, *supra* note 95.

120. *Id.*

121. Aloisi & De Stefano, *supra* note 89, at 298. *See also* Bennett Cyphers & Karen Gullo, *Inside the Invasive, Secretive 'Bossware' Tracking Workers*, EFF (June 30, 2020), https://www.eff.org/it/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers [https://perma.cc/Q756-3846].

122. This includes Skype, Cisco Webex, Google Hangouts, FaceTime, WhatsApp, Houseparty, and of course Zoom. *See* Naomi Fry, *Embracing the Chaotic Side of Zoom*, NEW YORKER (Apr. 20, 2020), https://www.newyorker.com/magazine/2020/04/27/embracing-the-chaotic-side-of-zoom [https://perma.cc/6PQF-FXL2].

123. Zoom is a videoconference platform that offers videotelephony and online chat services for free and through payment plans. It is considered to be extremely useful for people who work from home since it enables them to easily and virtually meet and chat with other people from all around the world. That is why the company launched a new category, "Zoom for home," which focuses on remote workers. *See About Us*, ZOOM, https://zoom.us/about [https://perma.cc/25AY-P292]; Jeff Smith, *Zoom for Home Is Here to Empower Remote Workers*, ZOOM (July 15, 2020), https://blog.zoom.us/zoom-for-home-empower-remote-workers [https://perma.cc/MXK8-3GXP].

124. Subrat Patnaik, *Zoom's Daily Participants Jumped from 10 million to Over 200 Million in 3 Months*, VENTUREBEAT (Apr. 2, 2020), https://venturebeat.com/2020/04/02/zooms-daily-active-users-jumped-from-10-million-to-over-200-million-in-3-months [https://perma.cc/AV89-4XPL].

125. Natalie Sherman, *Zoom Sees Sales Boom amid Pandemic*, BBC NEWS (June 2, 2020), https://www.bbc.com/news/business-52884782 [https://perma.cc/X39J-LTHX].

126. *See* Fry, *supra* note 122.

another arena of privacy infringement.[127] Zoom was suspected, at least in the past,[128] of providing employers with features aimed at supervising workers' online behavior without any explicit transparency of these features to users. According to a news report:

> Zoom's tattle-tale attention-tracking feature can tell your meeting host if you aren't paying attention to their meticulously-composed visual aids. Whether you're using Zoom's desktop client or mobile app, a meeting host can enable a built-in option which alerts them if any attendees go more than 30 seconds without Zoom being in focus on their screen. . . . If the feature is enabled on the account, a host can record the meeting along with its text transcription and a text file of any active chats in that meeting, and save it to the cloud where it can later be accessed by other authorized users at your company, including people who may have never attended the meeting in question.[129]

In many ways, the Zoom platform contains various surveillance capabilities similar to those of the time tracking programs. Yet, due to its supposedly "neutral" reputation, we are less aware of these far-reaching capabilities and their influence on teleworkers' right to privacy.[130]

In Part II.A.2, I will examine whether these various tracking programs—the explicit and the supposedly neutral ones—violate teleworkers' right to privacy. As part of this question, I will first examine what the right to privacy of employees contains. Thereafter, I will elaborate on the employer's rights

---

127. Since the Zoom platform is operated at the home-office and basically records and documents all activities that show up on the screen, teleworkers' family members can be caught within the frame and be watched by third parties. There are numerous examples, even well before the COVID-19 pandemic. One of the most memorable and funny is an online video interview of the political analyst and South Korea expert Robert Kelly on BBC. During the live interview, Kelly's two young children barged into the room, followed by their mother, who in panic pulled the children out of the room. This funny private moment was livestreamed to numerous people around the world and documented in the net forever. Similarly, once a Zoom meeting is being held in the hybrid home-office, where family members are present and may be caught by the Zoom camera in their habitual clothes or habits, the family members are also exposed to observation and even documentation by third parties. See the video at BBC News, *Children Interrupt BBC News Interview – BBC News*, YOUTUBE (Mar. 10, 2017), https://www.youtube.com/watch?v=Mh4f9AYRCZY [https://perma.cc/E8FB-KKWG]. *See also* Fry, *supra* note 122 (providing additional funny examples); Lynn, *supra* note 95.

128. Zoom's official announcement: "As of April 2, 2020, we have removed the attendee attention tracker feature as part of our commitment to the security and privacy of our customers." *Attendee Attention Tracking*, ZOOM, https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-Attention-Tracking [https://perma.cc/9T8C-YTQB].

129. Rae Hodge, *Using Zoom While Working From Home? Here Are The Privacy Risks to Watch Out For*, SFGATE (Apr. 2, 2020), https://www.sfgate.com/cnet/article/Using-Zoom-while-working-from-home-Here-are-the-15165641.php [https://perma.cc/3JU2-KNWX]; *see also* Karl Bode, *Working from Home? Zoom Tells Your Boss If You're Not Paying Attention*, VICE (Mar. 16, 2020), https://www.vice.com/amp/en/article/qjdnmm/working-from-home-zoom-tells-your-boss-if-youre-not-paying-attention [https://perma.cc/W3GV-J7GG].

130. Note that Zoom was sued in a class action lawsuit for some of its privacy violations. In April 2022, Zoom agreed to a settlement agreement of $85 million payout. Samantha Hawkins, *Zoom to Pay $85 Million in Deal Over User Privacy, 'Zoombombing'*, BLOOMBERG LAW (Apr. 22, 2022) https://news.bloomberglaw.com/privacy-and-data-security/zoom-to-pay-85-million-in-deal-over-user-privacy-zoombombing [https://perma.cc/FME8-29HG].

and interests in this case. On this basis, I will craft a legal balance between the employee's rights and the employer's prerogative, in the concrete case of supervising teleworkers in the home-office.

2. The Right to Privacy

Do these various modern tracking programs directed at the teleworker's work activity from home violate the worker's right to privacy? The right to privacy is important for the individual and society at large. However, in the workplace context, the right to privacy has a more limited interpretation, confined to protecting the employee's personal information, as long as the employee has made a reasonable effort to keep the information private.

The right to privacy has been interpreted in various ways over the years.[131] Privacy was famously conceptualized by Warren and Brandeis, back in 1890, as the right to be let alone.[132] The main objective of this right was to sustain a personal space where the individual is free from interference by others.[133] Privacy was also understood as a continuum from the individual's desire to stay in in her own protected realm, to the desire to be connected and exposed to others.[134] Privacy was similarly associated with the desire for control over one's information.[135] This notion of privacy is related to people's rights of autonomy[136] and dignity[137] and their right to determine for themselves if and how information about them will be exposed to others.

131. *See, e.g.*, Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193–96 (1890); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); H. J. Smith et al., *Information Privacy Research: An Interdisciplinary Review*, 35 MIS Q. 989, 992–96 (2011); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L. J. 421, 422-23, 428–29 (1980); Edward Shils, *Privacy: Its Constitution and Vicissitudes*, 31 L. & CONTEMP. PROBS. 281, 284 (1966); Michael Birnhack, *Domination and Consent: The Theoretical Basis of the Right to Privacy*, 11 L. & GOV'T 9, 13–14 (2008) (Hebrew); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1088–89, 1124–26 (2002); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 249–54 (2011); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1904–06 (2013); LESSIG, *supra* note 78, at 209–16.

132. *See* Warren & Brandeis, *supra* note 131. For a critical review of this article, see Matthew W. Finkin, *Employee Privacy, American Values, and the Law*, 72 CHI.-KENT L. REV. 221, 256–57 (1996).

133. Roger Clarke, *Internet Privacy Concerns Confirm the Case for Intervention*, 42 COMMC'N OF THE ACM 60, 60 (1999).

134. Smith et al., *supra* note 131, at 995. Also, for a discussion on the concept of possession or enjoyment of privacy, see Gavison, *supra* note 131, at 428–29.

135. WESTIN, *supra* note 131, at 13; H. J. Smith et al., *supra* note 134; James Rachels, *Why Privacy Is Important*, *in* PHILOSOPHICAL DIMENSION OF PRIVACY: AN ANTHOLOGY 290, 296–98 (Ferdinand D. Shoeman ed., 1984).

136. Warren & Brandeis, *supra* note 131, at 198; Shils, *supra* note 131, at 281–306. See also Matthew Finkin's discussion of the American Restatement of Employment Law, which connects the employee's privacy and autonomy. Matthew Finkin, *Chapter 7: Privacy and Autonomy*, 21 EMP. RTS. & EMP. POL'Y J. 589, 615 (2017).

137. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 971 (1964).

Privacy is also understood as part of the right to property.[138] Additionally, it is associated with political freedom of speech and beliefs[139] and even with the right to equality.[140] Privacy is linked to freedom of speech and equality mainly since, based on massive data collection, a violator may make a discriminatory decision against an individual in a way that may also violate that individual's right to be protected from discrimination or her right to freely express her political view.[141]

Alongside that, privacy is understood as being important for the community. Robert Post explains, in the context of privacy and the invasion of tort law, how privacy "does not simply uphold the interests of individuals against the demands of community, but instead safeguards rules of civility that in some significant measure constitute both individuals and community."[142] In a similar manner, Finkin explains how the desire for privacy is understood "as something that makes us human and is advanced as such."[143] He states that privacy is also important to the realization of other ends, mainly in order to enable the individual "to cultivate sufficient maturity to formulate and pursue life plans and to form independent moral and political judgments…without the distraction of being watched…and to be free from pressure to conform to popular, conventional standards."[144] This essentially means that *a community* must embrace the concept of privacy not only to protect human dignity and the autonomy of the individual member but also to protect the community's existence as a moral and democratic entity. The right to privacy can thus be viewed from a post-liberal perspective, which emphasizes its importance to the entire society as a common collective value.[145] According to this view, privacy is important in

138. On the connection between the right to privacy and other basic rights, see generally Frederick Davis, *What Do We Mean by "Right to Privacy"?*, 4 S.D. L. REV. 1 (1959); Gerald Dickler, *The Right of Privacy: A Proposed Redefinition*, 70 U.S. L. REV. 435 (1936); Harry Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 L. & CONTEMP. PROBS. 326 (1966); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

139. Alexander Hertel-Fernandez & Paul Secunda, *Citizens Coerced: A Legislative Fix for Workplace Political Intimidation Post-Citizens United*, 64 UCLA L. REV. DISCOURSE 2, 5–9 (2016) (focusing on the connection between privacy, data collection, freedom of speech, and employee beliefs in the digital virtual environment); *see also* Scott Skinner-Thompson, *Performative Privacy*, 50 U.C. DAVIS L. REV. 1673, 1676 (2017) (discussing political freedom in the surveillance state).

140. Richard Bruyer, *Privacy: A Review and Critique of the Literature*, 43 ALTA. L. REV. 533, 553, 587–88 (2006); Lisa Austin, *Privacy and the Question of Technology*, 22 L. & PHIL. 119, 144–45 (2003).

141. Bodie et al., *supra* note 79, at 1007–08.

142. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (1989).

143. Matthew W. Finkin, *The Surveillance Capitalism Controversy*, *in* PRIVACY E LAVORO, edited by Adriana Topo, Gianpiero Proia, and Carlo Pisani (forthcoming), at 37.

144. *Id.* (citing HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 75 (2010)).

145. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 148 (2004); PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 42–44 (1995); MARTA OTTO, THE RIGHT TO PRIVACY IN EMPLOYMENT 185–87 (2016). For a similar analysis

enabling individuals to maintain relational ties with one another and develop critical perspectives on the world in general.[146]

These common interpretations of the right to privacy are mainly associated with the protection of the individual from state surveillance.[147] Since the right to privacy was not an explicit part of the Constitution,[148] the Fourth Amendment[149] has been interpreted by the Supreme Court over the years as providing the individual a constitutional right against State intervention and only thereafter against other entities. Over time the right to privacy also grew to play an important role and to be justified in the specific context of the workplace.[150]

Similar to the way in which privacy is important for both the individual and the community at large, privacy is also important for the individual employee to enable her to enjoy some degree of autonomy at the workplace, to be protected from unjust discrimination by the employer, and to be able to express herself at work.[151] Moreover, privacy is considered to be important not only for individual employees, but also for employees as a distinct group. This is because the right to privacy rebalances the traditional prerogatives and capabilities of the employer to supervise employees as a group.[152] Privacy also enables a better redistribution of power between the employer and employees as part of the notion of distributive justice being one of the main goals of labor and employment law.[153]

---

of freedom of speech, particularly in the information society, see generally Jack M. Balkin, *The First Amendment is an Information Policy*, 41 HOFSTRA L. REV. 1 (2012).

146. Cohen, *supra* note 131, at 1906–07.

147. Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 744–47 (1989).

148. Finkin, *supra* note 136, at 610 (describing the Restatement of Employment Law, which refer to the right to privacy in the context of employees); Paul F. Gerhart, *Employee Privacy Rights in the United States*, 17 COMP. LAB. L. & POL'Y J. 175, 176–78 (1995); *see also* Steven L. Willborn, *Notice, Consent, and Nonconsent: Employee Privacy in the Restatement*, 100 CORNELL L. REV. 1423 (2015) (referring to the notion of employees' privacy in the Restatement of Employment Law).

149. The Fourth Amendment protects against unreasonable searches by government officials.

150. *See, e.g.*, Priscilla M. Regan, *Genetic Testing and Workplace Surveillance: Implications for Privacy*, *in* COMPUTERS, SURVEILLANCE, AND PRIVACY 21, 21–22 (David Lyon & Elia Zureik eds., 1996); Lucas D. Introna, *Workplace Surveillance, Privacy, and Distributive Justice*, 30 COMPS. & SOC'Y 33, 34 (2000).

151. *See generally* Ifeoma Ajunwa, *Protecting Workers' Civil Rights in the Digital Age*, 21 N.C. J.L. & TECH. 1 (2020); De Stefano, *supra* note 79, at 27-29.

152. Regan, *supra* note 150.

153. Introna, *supra* note 150, at 34–38; Guy Davidov, Distributive Justice and Labour Law, Lecture at the University College of London's Philosophical Foundations of Labour Law Conference (June 2016) (on file with author); Horacio Spector, *Philosophical Foundations of Labor Law*, 33 FLA. ST. U. L. REV. 1119, 1120, 1130–36 (2006); Guy Mundlak, *The Third Function of Labor Law: Distributing Labor Market Opportunities Among Workers*, *in* THE IDEA OF LABOR LAW 315, 316–17 (Guy Davidov & Brian Langille eds., 2011).

The right to privacy is part of U.S. employment law.[154] Yet, it has little meaning in the context of employment.[155] Since the right to privacy was originally understood as being applicable against state surveillance, the right to privacy is less consequential in the private sector even today.[156]

According to the Restatement of the Law of Employment, an employee has a right to privacy with regard to her personal information as long as she has made a reasonable effort to keep the information private.[157] In other words, when bringing a privacy violation claim, the employee must first prove that she has a reasonable expectation of privacy.[158] An employee has a reasonable expectation of privacy if she was given explicit notice from her employer that it considers the information at issue as private.[159] When the employer gives notice to the employee that it *does* supervise the employee's activity, the employer has a strong defense to a privacy violation.[160] In other words, according to Restatement of the Law of Employment, the right to privacy in the workplace mainly requires notifying the employee that she is supervised; it does not necessarily require her genuine agreement to such an intrusion.

This limited interpretation of privacy gained criticism from scholars.[161] According to the current legal landscape, however, it follows that there is a legal difference between teleworkers in the public sector and private sector with regard to the right to privacy. Since teleworkers in the public sector are supervised by the state (i.e., the government), not a private company, they supposedly benefit from a higher degree of protection of their right to

154. *See generally* Benjamin I. Sachs, *Privacy as Sphere Autonomy*, 88 BULL. COMP. LAB. REL. 233 (2014); Matthew W. Finkin, *Menschenbild: The Conception of the Employee as a Person in Western Law*, 23 COMP. LAB. L. & POL'Y J. 577, 586–90 (2002); Paul F. Gerhart, *Employee Privacy Rights in the United States*, 17 COMP. LAB. L.J. 175, 183–90 (1995); Rubenfeld, *supra* note 147, at 744-47.

155. Mainly in comparison to EU countries. *See* Matthew W. Finkin, *Pay Privacy in Comparative Context*, 22 EMP. RTS. & EMP. POL'Y J. 355, 359–60 (2018). For a comparative perspective on the right to privacy in the digital workplace, see Frank Hendrickx, *Protection of Workers' Personal Data: General Principles* 7-17 (ILO Working Paper 62, 2022), https://www.ilo.org/wcmsp5/groups/public/—-ed_protect/—-protrav/—-travail/documents/publication/wcms_844343.pdf [https://perma.cc/EB7P-3RRH].

156. *See, e.g.*, Jay P. Kesan, *Cyber-Working or Cyber-Shirking: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 293 (2002) (noting a lack of electronic privacy in the workplace); Shlomit Yanisky-Ravid, *To Read or Not to Read: Privacy Within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory*, 64 AM. U. L. REV. 53, 87–88 (2014) (discussing the lack of legal protections against employer electronic surveillance of emails, mobile phones, etc.).

157. Finkin, *supra* note 136, at 603.

158. *Id.* at 593. In contrast, when an employer intrudes on the physical person and possessions of the employee, "a legally recognized privacy interest is accorded per se and analysis turns to the actionability for an infringement of it." *Id.*

159. Finkin, *supra* note 136, at 597.

160. *Id.* at 597-98. For a critical view of this state of things, see generally Willborn, *supra* note 148.

161. *See* Finkin, *supra* note 136, at 597; *see also* discussion *infra* Part II.A.4.

privacy.[162] It also seems that the employer can in certain cases avoid responsibility for a privacy violation if it notifies the employee that she is being supervised.

3. The Employer's Interests and Prerogatives

The economic interests and property rights of the employer stand against the employee's right to privacy.[163] In the context of telework, other employer's justifications lie in opposition to employees' privacy interests. Among them are the economic interests of the employer to ensure that the worker is actually working from distance, questions of cybersecurity and the employer's rights and responsibilities with regard to protected information, and the employer's duty to ensure that the worker is working in accordance with lawful timelines rather than working unauthorized overtime hours.

According to the Restatement (Second) of Employment Law, the employee seemingly does not have a right to privacy in regard to "information that is relevant to the company's business needs."[164] Therefore, an employer can argue that unlike in the office—where the worker's manager and colleagues can verify that the worker is actually working—in the home-office, the only way the employer has to verify that the worker is actually working is by using tracking programs.[165] In other words, the employer can argue that since employees are being paid for their working time, employers have a "business need" to monitor them to determine that they are truly working at home rather than using the time to conduct private activities.[166]

In this way, when the information on an employee relates to her physical or electronic location—for instance, from a program whose purpose is to determine whether the employee sits near her computer or stays at home—the employer can argue that it has the right to verify that the employee actually stays at home and works during scheduled working hours for which she is being paid.[167] The employer can similarly argue that it uses tracking program targeting the worker's keyboard strokes, mouse movements, and websites visited, or software that takes random screenshots of the worker's computer or face, to ensure that the worker actually works in front of the computer and uses her computer for only the employer's business needs. This is a stronger argument when the employee has been given notice that a

162. *See* Finkin, *supra* note 136, at 596; Rogers, *supra* note 79, at 550; Pauline T. Kim, *Market Norms and Constitutional Values in the Government Workplace*, 94 N.C. L. REV. 601 (2016).

163. Finkin, *supra* note 136, at 592–93.

164. *Id.*

165. *See* discussion *supra* note 92. Note that employers can make the same argument when the monitoring is being done in the workplace. *Cf.* Ball, *supra* note 73, at 90–93.

166. Finkin, *supra* note 136, at 592; *see also* Mosendz & Melin, *supra* note 95.

167. *See, e.g.*, Hugh Collins, *The Right to Flexibility*, *in* LABOUR LAW, WORK, AND FAMILY 99 (Joanne Conaghan & Kerry Rittich eds., 2005).

tracking program was installed on the employee's devices, and stronger yet when the employee is the one who installed the program at the request of the employer and thus appears to have agreed to it.[168]

To this we need to add all the various programs that score the worker's activity based on her online activity and compare her rating to that of other workers, as well as the programs that encourage more communication between workers by potentially constantly recording them.[169] An employer can argue that the business has an interest not only to verify that the worker is actually working but also to encourage the worker to work faster, to be more productive, and to communicate with colleagues. An employer can argue that it must use these tracking programs for these purposes precisely because in the telework case each worker is isolated, both from the employer and their colleagues, so other means to ensure "healthy" competition and better collaboration among workers are needed.[170] These two first arguments—assuring that the employee is actually working and assuring the employee's productivity—are an integral part of the employer's prerogatives to run her business and manage her employees.

Additionally, an employer can assert that it must monitor the employee from a distance to ensure that there are no security breaches by the employee or any security risks to the company's data.[171] As various research demonstrates, the shift to telework during the pandemic has led to an increase in the number of cyberattacks on firms' data and on personal computers.[172] Other research shows an increase of 600% in phishing as a consequence of the pandemic in March 2020.[173] This reflects pre-COVID findings from recent years that show an increasing number of cybersecurity risks when workers work from home.[174] A good example of this can be found in Bispham

168. As was explained in *supra* notes 157–160 and accompanying text.

169. As was described in *supra* notes 117–120 and accompanying text.

170. Compare the discussion of these tracking programs *infra* Part II.A.1.

171. *See, e.g.*, *Is a Hybrid Workforce Putting Your Cybersecurity at Risk?*, INSIGHT (July 7, 2021), https://www.insight.com/en_US/content-and-resources/gated/is-a-hybrid-workforce-putting-your-cybersecurity-at-risk-ac1246.html [https://perma.cc/VBM3-ZGW5]. Needless to say, employers can make the same argument when the monitoring is being done in the workplace. *Cf.* Ball, *supra* note 73, at 90–93.

172. *See, e.g.*, Arnold Mashud Abukari & Edem Kwedzo Bankas, *Some Cyber Security Hygienic Protocols for Teleworkers in COVID-19 Pandemic Period and Beyond*, 11 INT'L J. SCI. & ENG'G RSCH. 1401, 1401–02 (2020); PONEMON INSTITUTE, CYBERSECURITY IN THE REMOTE WORK ERA: A GLOBAL RISK REPORT 1–3 (2020), https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf [https://perma.cc/WYK4-62GR]; Luke Irwin, *The Cyber Security Risks of Working from Home*, IT GOVERNANCE (Aug. 19, 2021) https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home [https://perma.cc/AN4C-2FML]; Mary Bispham et al., *Cybersecurity in Working from Home: An Exploratory Study*, 1–2 (Aug. 1, 2021).

173. Bispham et al., *supra* note 172, at 6.

174. C. E. Medina-Rodríguez et al., *The Cyber Security in the Age of Telework: A Descriptive Research Framework Through Science Mapping*, International Conference on Data Analytics for Business

et al., which shows that "countries with a higher percentage of employees WFH [working from home] are allocated in the top half of the countries with a larger percentage of users experiencing cybersecurity incidents in 2019."[175]

Thus, an employer can argue that it must monitor employees from distance to prevent them from copying a confidential client list from the company's data;[176] to prevent defamation, sabotage of data, and data theft and hacking;[177] to test and assure the security of the company's systems from cyberattack by others;[178] to prevent vulnerabilities in video-conferencing platforms, such as "Zoom bombing," in which a malicious user "bombs" a meeting by sharing vulgar images;[179] or to prevent home-office teleworkers from exposing confidential information to other people who live with them. As will be shown in the following parts, it is doubtful whether and how much the current monitoring programs from a distance actually promote cyber security. Many times, it appears that the opposite is true.

Finally, and perhaps much less believably, the employer can argue that it wishes to constantly supervise the employee from a distance to ensure that the employee is not working more than the required working hours and her right to rest time is being preserved as she works from home.[180] Generally speaking, this argument is most used in the EU, where working time

---

and Industry: Way Towards a Sustainable Economy, at Section V – Conclusions (2020), https://ieeexplore.ieee.org/document/9325633 [https://perma.cc/Q2DN-SAPL] ("The size of literature related to Telework and Cyber Security shows a remarkable increase in the last years. Given the large volume of citations received in this field, the growth of literature is expected to continue in the coming years.").

175. Bispham et al., *supra* note 172, at 3.

176. *See* Mosendz & Melin, *supra* note 95.

177. Ball, *supra* note 73, at 93.

178. See, for example, The Investigatory Powers (Interception by Businesses Etc. For Monitoring and Record-Keeping Purposes) Regulations 2018, Explanatory Memorandum ¶ 7.4 (UK), which allows certain public authorities in the United Kingdom to intercept communications for reasons of national cyber-security.

179. Bispham et al., *supra* note 172, at 7; *see also* Hodge, *supra* note 129 (chronologically detailing numerous cases of such break-ins); Tom Warren, *Zoom Faces a Privacy and Security Backlash as it Surges in Popularity*, THE VERGE (Apr. 1, 2020), https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response [https://perma.cc/D3BN-HL6W]. Note that an April 2020 special report issued jointly by the Department of Homeland Security's Cyber Mission and Counterintelligence Mission Centers argues that Zoom is vulnerable to intrusions by foreign government spy services. *See* Josh Margolin, *Intel Report Warns Zoom Could Be Vulnerable to Foreign Surveillance*, ABC NEWS (Apr. 28, 2020), https://abcnews.go.com/International/intel-report-warns-zoom-vulnerable-foreign-surveillance/story?id=70376203 [https://perma.cc/387C-36WD].

180. EUROFOUND, RIGHT TO DISCONNECT: EXPLORING COMPANY PRACTICES 45–47 (Publications Office of the European Union, Luxembourg, 2021), http://www.bollettinoadapt.it/wp-content/uploads/2021/09/ef21049en.pdf [https://perma.cc/8JWK-NJAX].

limitations are preserved.[181] However, there might be cases in which an employer will make such an argument in the United States as well.[182]

4. Between the Employee's Privacy and the Employer's Prerogatives

So far, we have examined the employee and employer's rights and interests that are at stake when dealing with the right to privacy of employees in the home-office. Seemingly, the employer can argue that she has meaningful interests when an employee works from a distance that might diminish the employee's right to privacy. However, the tremendous developments in tracking programs and their far-reaching abilities to monitor the activity of an employee in her private home raise many privacy concerns. Due to the many new scenarios and threats that modern life has thrust against the concept of privacy in the labor context, numerous scholars call for a broader interpretation of the right to privacy of all employees, whether they are in the public sector or the private sector.[183] A broader and more up-to-date interpretation of the right to privacy could ensure an authentic protection of this right in the modern labor market, including in the telework case.

In other words, the current legal balance between the employer's economic interests and the employee's right to privacy tilts the scale in the direction of the employer's economic interests at the expense of the employee's right to privacy. This reality has gained a lot of criticism from various scholars throughout the years, particularly on the background of the digital reality and the new technological innovations it has brought with it.

In his comprehensive work on the right to privacy in employment law, Finkin argued, against the backdrop of the modern smart technology, that the traditional limited interpretation of employees' privacy may severely infringe employees' rights.[184] He demonstrated how the traditional interpretation of privacy is anachronistic and does not correspond with the various new threats

181. See, for example, the situation in France, Spain, Italy, and Germany, as described in Katsabian, *supra* note 14, at 393-99; *see also* EUROFOUND & INT'L LAB. OFF., *supra* note 24, at 50-51; Andrew Pakes, *The Right to Disconnect*, IFOW (Apr. 16, 2021), https://www.ifow.org/news-articles/the-right-to-disconnect [https://perma.cc/5EDC-M5F7]; Tom Bateman, *Portugal Makes It Illegal for Your Boss to Text You after Work in 'Game Changer' Remote Work Law*, EURO NEWS (Nov. 11, 2021), https://www.euronews.com/next/2021/11/08/portugal-makes-it-illegal-for-your-boss-to-text-you-after-work [https://perma.cc/TGW6-5A2P].

182. For other possible justifications employers might use to monitor their employees from a distance, see Vatcha, *supra* note 92, at 5 ("Employers justify carrying out surveillance to protect company secrets and sensitive confidential information, protect themselves in case of liability issues such as discrimination or harassment, prevent 'time theft' where employees lie about their hours, discourage employees from carrying out non work related tasks at work, or 'careless communication' which can expose the company's systems to phishing.").

183. *See, e.g.*, MARTA OTTO, THE RIGHT TO PRIVACY IN EMPLOYMENT 185-87 (2016). For a similar argument regarding digital reality, see Nissenbaum, *supra* note 145, at 137–38; *see also* Miriam A. Cherry, A *Taxonomy of Virtual Work*, 45 GA. L. REV. 951, 991–92 (2011) (comparing the right to privacy in the United States and Europe and the need to develop it further in the former).

184. Finkin, *supra* note 136, at 620–21.

the concept of privacy faces today.[185] In a similar manner, Ajunwa, Crawford, and Schultz showed that the ability of the employer to vet its employees beyond the limitations of working time and space has dramatically increased during the digital revolution.[186] The relevant laws that deals with privacy violation, however—enacted primarily at the federal level as anti-discrimination laws, and in several states as well—were mainly developed before the digital revolution and cannot provide a satisfactory solution to the various new privacy violations we encounter today.[187] Since the issue of privacy in the modern workplace is more complex than current laws that deals with privacy, Ajunwa, Crawford, and Schultz suggested that a sector-specific approach toward privacy in the employment context should be developed that takes into consideration the unique employee–employer power dynamics in the digital reality.[188] Similarly, Rogers showed how current workplace privacy laws should give employees real protection against the numerous sophisticated technological surveillance tools in existence today. [189] In practice, however, these laws give workers very few protections that can truly deter their employers from excessively supervising them. Given these realities, Rogers suggested a comprehensive solution of democratizing the modern workplace in a way that ensures the protection of the employee's right to privacy.[190]

Applying these understandings in the context of the new sophisticated surveillance tools, we can see that these tools might be allowed under current privacy laws, but this is so only because the laws are not progressive enough and do not provide real protection to workers' right to privacy in the modern age.

This understanding intensifies when we consider the uniqueness of the hybrid home-office. Unlike the familiar discussions about privacy in which the monitoring initially seems to apply within the physical limitations of the workplace yet can easily reach to the private sphere of the individual, in this context *by definition* the program is used to vet the teleworker at her private home. It is much easier for the employer to access vast amounts of private information about teleworkers who use their personal devices to conduct

185. *Id.*

186. Ajunwa et al., *supra* note 75, at 742–46; *see also* Katsabian, *supra* note 19, at 212–16.

187. *See* Ajunwa et al., *supra* note 75, at 747–62.

188. *Id.* at 774–75 (suggesting that "a hypothetical 'Employee Privacy Protection Act' (EPPA) could specifically limit workplace surveillance to its appropriate context—actual workplaces and actual work tasks.").

189. Rogers, *supra* note 79, at 544–53; *see also* Cherry, *supra* note 183, at 991–93 (criticizing the U.S.'s comparative lack of employee surveillance protections and discussing the greater threat to privacy in virtual work environments).

190. Rogers, *supra* note 79, at 576–83 (arguing that the ideal solution would raise minimum standards and expand the scope of employment, share data to encourage enforcement and organizing, and encourage organizing and bargaining around technological choices).

work from home when the tracking program is installed on the teleworker's *own private* mobile phone or laptop. Thus, when dealing with the home-office, the line between the employee's private activity and behavior and her professional activity and behavior is, by definition, being blurred.[191] Since this involves private electronic devices that contain private information and that are in the physical private sphere of the teleworker, using tracking apps inevitably leads to a privacy violation of greater intensity and scope than can occur with common supervision in the workplace. At the workplace, mainly due to long working hours, it seems reasonable to assume that most of us check our bank account or look at an email we received from our doctor without being so exposed to the employer's constant supervision. The absurdity is that in their own homes, teleworkers are much more exposed to constant and intrusive monitoring by their employers.

To this absurd reality, we need to add that some employers can use this private information on the employee that was collected on her in her private home for improper purposes. The most egregious example is to harass an employee sexually—i.e., to gain the employee's personal information to learn about her intimate private reality or to sexually threaten her based on this personal information.[192] Alongside that, sometimes employer's accumulated employee data is unintentionally leaked to third parties who can use it for unlawful purposes.[193]

This is particularly problematic given that these programs are seemingly here to stay, even after the COVID-19 pandemic is over.[194] Once the company has acquired and paid for a tracking program and demanded that the employee install it on her computer, it is unlikely that the company will ask the employee to remove the program when she continues to occasionally telework from home. Later, this Article will elaborate on how this new state of things should change the current balance between employee's right to privacy, particularly when they work from home, and the employer's interests and needs. However, first, it is important to mention another important factor that emerges from the descriptions presented so far: the implications of the current monitoring programs for the right to privacy of

191. *Cf.* Katsabian, *supra* note 14 (arguing that this home-office reality inevitably blurs the line between the teleworker's leisure time and rest time).

192. For more information on the commonality of sexual harassments and its far-reaching problematic outcomes, see Lilia M. Cortina and Maira A. Areguin, *Putting People Down and Pushing Them Out: Sexual Harassment in the Workplace*, 8 ANN. REV. ORGANIZATIONAL PSYCH. AND ORGANIZATIONAL BEHAV. 285, 291–95 (2021).

193. See *supra* notes 171–179 and accompanying text for prior discussion of cybersecurity risks, applied now to data collected by employers.

194. Heaven, *supra* note 16 (statement of Tommy Weir, CEO of Enaible) ("I think workplace monitoring is going to become mainstream."); *see also* Lynn, *supra* note 95 (discussing ongoing problems with invasive monitoring technology).

third parties, including minors, and the involvement of third parties as privacy violators.

B. Third Parties as Privacy Violators

Along with more intensive intrusion into the teleworker's private life, teleworking from home emphasizes the ability third parties have to influence privacy in the labor context and the negative side effects the supervision of teleworkers may have on third parties. When an employer requires a teleworker to install a tracking app on her private devices in her home-office, third parties associated with the supervision task—such as those creating the tracking technology—also play a role in violating the teleworker's right to privacy.

Arguably, because of inequality of the bargaining power of the employer and employees, the employer should bear sole responsibility for violation of the employee's rights. However, in recent years, scholars have argued that tech companies should also have ongoing responsibility for the products they generate and their implications for society.[195] This seems particularly true with respect to the right to privacy: when a company develops a program that clearly has negative implications for the right to privacy, the company also has some responsibility for privacy violations enabled by the program, and it needs to design the program differently to ensure the protection of human rights.[196] Similarly, in the labor context, Poster argued with respect to the extensive surveillance culture in transnational call centers that other entities, beyond the employer, should be responsible for violation of employees' privacy.[197] Among them are, first and foremost, the producers and programmers in tech companies, who "have a crucial role in the process: they define the parameters of what is being surveilled, they create the techniques for carrying it out, and they lay the groundwork [for] multisurveillance."[198]

Transnational call centers are similar to teleworking in the sense that the employer is geographically remote from its employees and searching for alternative virtual ways to supervise them.[199] Based on Poster's argument and the notion of the social responsibility of programmers and tech companies, then, tech companies are integral to increasing and sustaining the surveillance of teleworkers. This is so because of the continual advancement of the

195. *See generally* Michael E. Porter & Mark R. Kramer, *Strategy & Society: The Link Between Competitive Advantage and Corporate Social Responsibility*, 84 HARV. BUS. REV. 78 (2006) (calling for a reimagined strategy for implementing corporate social responsibility).

196. *See generally* Irene Pollach, *Online Privacy as a Corporate Social Responsibility: An Empirical Study*, 20 BUS. ETHICS: A EUR. REV. 88 (2011).

197. WINIFRED R. POSTER, MULTI-SURVEILLANCES TRANSNATIONAL DIGITAL AGENCIES IN THE OUTSOURCED SERVICES OF INDIAN CALL CENTERS 37–56 (forthcoming).

198. *Id.* at 37.

199. Call centers are located in a different country than the one in which the firms that use call center services are located.

surveillance capabilities of the programs they produce—from counting working hours to taking random screenshots of the worker's computer to video recording the worker's screen to scoring the worker based on her online behavior to even offering the employer methods to speed up the worker's work. These companies not only create a concerning environment of privacy violations, but they also have access to some of the accumulated data. This is mainly true for online programs that use AI to process data and create a productivity report for the employer based on that data. Such companies may use the collected private data to refine and improve the activity of the AI program.[200] Then, with an enhanced AI program, they expose employees to further intrusion by a third party.[201]

C. Third Parties as Victims: The "Side Effect" of Supervision of Teleworkers

Just as entities other than employers are offenders in surveillance of teleworkers, other people, in addition to teleworkers, are its victims. Since the program aims to track every activity of the teleworker during her working time, every person who was involved in any such activity, in whatever way, is in the net of supervision by the employer. This is true first and foremost of family members, who might use the same private technological devices on which the tracking program was installed; their activities are also exposed to and documented by the employer. Family members can also be caught, somewhere in the background, in random photographing of the worker.[202] A good example of that can be found in Satariano's article, which is accompanied by a short video of his activity during his workday created by the tracking program. Most of the time, we see Satariano working at his computer. However, because the video runs for several hours, his children are also exposed in it; their faces and activities are filmed in the background and documented.[203]

Similarly, in the Teleperformance's workers case in Colombia and Albania, other parties were exposed to the employer's supervision, among them the workers' partners who shared with them a working space (or bedroom) in which a camera was installed.[204] For this exact reason, the company required the workers to sign an agreement by which the worker

200. This phenomenon is defined as "machine learning" or "data analytics." *See* Rogers, *supra* note 79, at 556–58; Matthew Scherer et al., *Applying Old Rules to New Tools: Employment Discrimination Law in the Age of Algorithms*, 71 S.C. L. REV. 449, 453–56 (2019); Bodie et. al., *supra* note 79, at 964–65; Hirsch, *supra* note 79.

201. The problem lies in the fact that the third-party companies can obtain and store the collected data, not necessarily in the suspicion that they watch or are exposed to it.

202. *See supra* note 106 and accompanying text.

203. Satariano, *supra* note 95.

204. Solon, *supra* note 94.

agreed to share data and images related to the worker's children under the age of eighteen who might get picked up by video and audio monitoring tools.[205] This shows that the company is well aware that the monitoring process might invade the right to privacy of others, including minors, and seeks contractual ways to avoid legal responsibility for such an infringement.

Other people can also be tracked by tracking programs. In the above-mentioned testimony of Satariano, a screenshot caught "the trainer setting up to teach the class in her living room."[206] This demonstrates the ease with which the activity of a person in her own home who is not associated with the teleworker's workplace and never gave her permission for this sort of documentation is exposed to the employer's monitoring. Satariano's supervisor describes how she was also exposed by the program to "dozens of screenshots includ[ing] those of a Google Meet conference call that Adam had participated in, which displayed as extremely close-up photos of the faces of numerous colleagues."[207] These people were not necessarily associated with Satariano's workplace, and they were probably not aware of the supervision—and yet, they were exposed to it. Hypothetically, and even more intrusively, Satariano's employer easily could have been able to see private correspondence or files of a third party that were sent to Satariano and caught in a random screenshot. Such private activity could be documented in the employer's files forever.

The implications of this are troubling. Because of the way work is conducted in the hybrid home-office, endless third parties who interact with the teleworker, physically or virtually, are exposed to the supervisory eye of the employer. These third parties are not professionally related to the employer. They probably do not know the people responsible for the surveillance by the employer. They did not agree to this kind of intrusive monitoring. They are not even aware of it. Some of them are minors. Nevertheless, the increasingly common phenomenon of monitoring and filming teleworkers at their home-office can violate their right to privacy.

III. THE QUESTION OF REGULATION

Intensive intrusions into the teleworker's private sphere in the name of professional and business motivations have dramatically affected the teleworker's right to privacy. Due to the hybrid nature of the home-office, the potential for a privacy infringement is bigger when the work is being conducted from home. The intrusive supervision of teleworkers intensively involves third parties, both as violators and victims. Against the background

205. *Id.*
206. Satariano, *supra* note 95.
207. *Id.*

of this reality, this Part proposes principles to address the privacy challenges of telework.

Since the main source of the privacy challenge is rooted in the private-public assimilation, an effective model of regulation should contain various elements that also refer to this assimilation. Effective regulatory principles should thus deal with the employer's direct actions that violate the employee's right to privacy as well as with the external mechanisms that the employer uses to supervise her employees outside the limitations of the physical workplace. In other words, since privacy violations in the home-office are possible due to the emergence of dubious surveillance programs developed for this purpose, the companies that produce these programs are also part of the problem and should be included in any solution model. Similarly, effective regulatory principles should refer to both the employee's right to privacy as well as the right to privacy of third parties when they interact with the teleworker in the private domain. Since we are dealing with the question of privacy in the employment context, the specific power dynamics, rights, and needs of both the employee and the employer should also be taken into consideration.

To effectively deal with the privacy difficulty in the hybrid home-office, a hybrid solution should be used; a solution that encompasses both employers and the tech industry, both employees and those around them, in the specific context of the workplace. In the following pages, this Article will first discuss the responsibilities and prerogatives employers should have. Thereafter, it will discuss the responsibility tech companies should have to protect the right to privacy of employees and others when developing tracking-from-distance programs.

A. The Proportionality Approach

As discussed earlier, the employer's economic interests and rights stand against the employee's right to privacy. Using monitoring programs in the hybrid home-office tilts the scale in the direction of the professional interests of the employer at the expense of the employee's right to privacy. This is true because the monitoring programs enable the employer to easily access vast amounts of private information on the employee and others around her, even when the information is not necessarily required to protect the company's economic interests.[208] This reality must also be understood against the background of the workplace context and the unique unequal power dynamic between the employer and the employee, in which the employer has an a priori extensive power, in the economic and psychological meanings, over

208. *See* discussion *infra* Part II.A.1.

the employee.[209] Thus, the violation of the employee's right to privacy appears to have even more far-reaching implications on the employee's well-being and rights when she is also economically and emotionally dependent on her employer and the workplace.

As discussed, many privacy laws are outdated and insufficient to deal with the various new challenges that technology is bringing to the labor field.[210] This is also true with respect to telework. In some countries, due to the importance of privacy in the employment context, employers are banned from supervising their employees while they are working from home.[211] In the United States, it is doubtful that such an absolute rule will ever be applied when the employer's interests are at stake.[212] However, if we want to rebalance the employee-employer equation and ensure that the employee's right to privacy is not being unjustifiably manipulated and obliterated by the employer, the business needs of the employer must be considered proportionately. In other words, the main and basic regulatory principle in this case should be one of proportionality.[213]

The proportionality principle is applied in numerous countries around the world and is considered a leading judicial principle in many of them.[214] In the United States, it seems that this principle has been implicitly implemented in diverse canonical decisions, mainly in constitutional law.[215] The proportionality principle determines whether a specific violation of the rights or interests of an individual is proportional and therefore valid. A

209. *See generally* Guy Davidov, *The Three Axes of Employment Relationships: A Characterization of Workers in Need of Protection*, 52 UNIV. OF TORONTO L. J. 357, 365–76 (2002) (describing court tests for control/subordination and economic dependency to determine status as employee or independent contractor); Gali Racabi, *Abolish the Employer Prerogative, Unleash Work Law*, 43 BERKELEY J. EMP. & LAB. L. 79 (2022) (criticizing the employer prerogative's dominance over the American workplace).

210. *See supra* notes 185–190 and accompanying text.

211. For instance, this is the case in Portugal. *See* Bateman, *supra* note 181.

212. *See* discussion *infra* Part II.A.3.

213. GUY DAVIDOV, A PURPOSIVE APPROACH TO LABOUR LAW 186 (2016) [hereinafter Davidov, PURPOSIVE APPROACH]; Katsabian, *supra* note 19, at 236–37.

214. DAVID M. BEATTY, THE ULTIMATE RULE OF LAW 162 (2003) (referring to the proportionality principle as the "ultimate rule of law" and demonstrating its use in diverse legal systems worldwide). For proportionality in EU privacy regulation, see also Hendrickx, *supra* note 155, at 26–27.

215. BEATTY, *supra* note 214, at 162–63, 175–88. *See also* Vicki C. Jackson, *Constitutional Law in an Age of Proportionality*, 124 YALE L. J. 3094, 3096 (2015) ("The United States is often viewed as an outlier in this transnational embrace of proportionality in constitutional law. Yet some areas of U.S. constitutional law embrace proportionality as a principle, as in Eighth Amendment case law, or contain other elements of the structured 'proportionality review' widely used in foreign constitutional jurisprudence, including the inquiry into 'narrow tailoring' or 'less restrictive alternatives' found in U.S. strict scrutiny."); Eric Engle, *The History of the General Principle of Proportionality: An Overview*, 10 DARTMOUTH L.J. 1, 7–9 (2012) (identifying the proportionality principle in U.S. constitutional law); Moshe Cohen-Eliya and Iddo Porat, *Proportionality and the Culture of Justification*, 59 AM. J. COMP. L. 463, 465 (2011) (explaining that the U.S. Supreme Court is the exception to widespread adoption of proportionality, but there "have been some attempts to introduce a form of this doctrine into U.S. constitutional law as well.").

decision is proportional if it meets three criteria: (1) there is a rational connection between the goal and the means utilized by the law to achieve it, (2) there are no other possible and less restrictive means of achieving the goal, and (3) there is a proportionate balance between the benefit of achieving the goal and the damage that may be caused to the rights of the individual.[216]

Over the years, the proportionality principle has been applied in the field of labor and employment law, including specifically with regard to the right to privacy.[217] Accordingly, in the context of teleworkers' right to privacy, to decide whether the violation of an employee's right to privacy was proportional or not, the three secondary criteria should be analyzed to balance the specific rights and interests at stake. In other words, it should be determined whether (1) there is a rational connection between the goal being furthered by teleworkers' supervision and the means of accomplishing it, (2) the least restrictive means of achieving the employer's goal were used, and (3) there is a proportionate balance between the social benefit of achieving the employer's goal and the harm that may be caused to the teleworker's and their surroundings' right to privacy.[218]

For the first criterion, the premise is that employers intrusively supervise their employees at home to verify that they spend their working time on work and to reduce any security risks posed by the teleworker herself or by third parties.[219] However, it is doubtful whether the various new programs that score the worker's activity based on her online activity and compare it to that of other workers accomplish this business interest.[220] These AI programs mainly aim to speed up the teleworker's activity and reward or punish her for productive or nonproductive activity. These are not aimed at ensuring that the teleworker actually works during their working time. In a similar manner, and even more explicitly, it is questionable whether and how taking random screenshots or videos of the employee during her workday or scoring the employee's activity actually prevents cybersecurity risks.

Similarly, considering the second criterion, it is questionable whether these AI programs, along with taking random screenshots of the worker's computer every couple of minutes, taking videos of the worker's screen or face every ten minutes, or monitoring all the employee's emails and social

216. *See* Aharon Barak, *Proportionality and Principled Balancing*, 4 L. & ETHICS HUM. RTS. 2, 4–6 (2010).

217. Davidov, PURPOSIVE APPROACH, *supra* note 213, at 186; *see also* Guy Davidov, *Comments on the Issue of Online Privacy at the Workplace, Multi-Disciplinary Workshop on Privacy in a Digital Environment at the Hebrew University of Jerusalem* (Dec. 2003) (Hebrew) [hereinafter Davidov, *Comments*]; Eusebi Colàs Neila, *Fundamental Rights of Workers in the Digital Age: A Methodological Approach from a Case Study* 27–29, 33–47 (Centro Studi di Diritto del Lavoro Europeo "Massimo D'Antona", Working Paper No. 89, 2011).

218. Davidov, *Comments*, *supra* note 217.

219. *See infra* Part II.A.3; *see also* Mosendz & Melin, *supra* note 95.

220. *See* review of score-generating programs in *supra* notes 116–120120 and accompanying text.

media usage, could be considered "the least restrictive means of achieving the employer's goal." There are other ways of ensuring that a remote worker is indeed working and reducing security risks that do not involve such extreme and constant violations of privacy of the employee and of third parties. One such way would be providing the employee with the devices required for work (for example, a laptop and a mobile phone), on which the employer could install the least-intrusive monitoring programs. This type of solution would ensure separation of the employee's personal data installed on her private devices (not to mentioned personal data of the employee's family members) and the professional data of the employee on employer-provided devices.[221] Since the least-intrusive monitoring programs should be installed on the professional equipment, it should not include taking pictures of the employee, which cause the greatest violation of the right to privacy of the employee and that of her family members and anyone who physically or virtually connects with her. In another context, I offered to develop a remote calculation model that monitors the employee from a distance based on her constant notice and consent.[222] Such a model can ensure that the employers' interests and needs are being preserved without using a harmful monitoring tool. Another way can be to document distinct private web pages the employee has been visiting for extended periods (without exposing the content of the page), or to delete the accumulated data at the end of every day.

Finally, the third criterion—ensuring a proportionate balance between the benefits to the employer and the harm to the employee's and others' right to privacy—has not been followed at all in the current environment. It is doubtful whether the right to privacy of third parties, especially minors, should be balanced against the employer's economic interests at all. As explained above, these third parties are not directly connected to the workplace and may be unaware of the privacy violation. Thus, the employer would have to provide a strong justification for why violating their rights is justified and proportional. Indeed, some employers demand that the

221. *See* Ifeoma Ajunwa, *Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law*, 63 ST. LOUIS U. L.J. 21, 49–50 (2018) (showing that courts have found that employees do not have a reasonable expectation of privacy when using employer-owned technology).

222. The suggestion, made to count the actual working hours of the worker from a distance, was also for the worker's benefit. According to this suggestion, "the remote calculation will initially only be exposed to the person who conducts the work from a distance (i.e., the employee). In cases when the program identifies that the employee is conducting work outside of the workplace, during the employee's supposed leisure time, then the program can, for instance, send the employee a pop-up message, asking them whether they are conducting work and wish to calculate it as working time. If the employee's answer is positive, then the employer will have access to the specific content in accordance with privacy rules (as the employer does to professional content produced in the workplace during working hours). To ensure that the employee is aware of this, each time the employee's answer is positive, the program will automatically, briefly, and clearly notify the employee of the meaning of their consent and of the exact content to which the employer will have access." Katsabian, *supra* note 14, at 411.

employee herself intrude upon the right to privacy of her family members, including minors.[223] However, since these third parties are not under the authority of the workplace and are not subject to the employer's orders and prerogatives, it is not clear at all how the employer can validly reduce their rights through a forced agreement by the employee.[224] In any case, this sort of decision has to be proportional and take into consideration the fact that these third parties are not at all a part of the employer's prerogatives.

As for the balancing equation between the employer and the employee herself, in the current employer-employee relationship—in which the employer is the sole determiner of whether to use a monitoring program and, if so, which one, when, and how—it is questionable whether there could be a genuine proportional balance between the rights and interests of the two sides. To be sure, employers face a challenge in managing a workplace when work is being conducted from distance. But today, the employer's interests are the *only* interests that are considered.[225] Therefore, to ensure that workers' needs and rights are also taken into account, and that there is a proportional balance between the two sides, it is important to give a meaningful role and voice to employees' representatives. One way to do so is by the employer generating a privacy policy together with employees' representatives. I will expand upon this point in the following Part.

B. A Privacy Policy

To ensure that the third criterion of the proportionality approach is being met, the law should require employers to generate a privacy policy for teleworkers, in the specific workplace, with the involvement and agreement of workers' representatives.[226] Such a workplace-based privacy policy can

223. *See supra* notes 204–205196 and accompanying text.

224. *Cf.* Angus Thompson, *A Workspace is a Workspace: Council Banned Staff Supervising Kids While Working from Home*, SYDNEY MORNING HERALD (July 8, 2021), https://www.smh.com.au/national/nsw/a-work-space-is-a-work-space-council-banned-staff-supervising-kids-while-working-from-home-20210708-p587vo.html [https://perma.cc/W3XD-KZ9G] (describing an employer requirement from the city counsel of Sydney, Australia that employees sign declarations that they would not supervise their children while working with the purpose of enforcing a work-only policy during work hours).

225. *Cf.* Ajunwa et al., *supra* note 75, at 742–46 (discussing employer justifications for privacy invasions on the basis of improving efficiency and innovation); Rogers, *supra* note 79, at 535 (describing how employers are developing automation and "Algorithmic Management" technology that subjects employees to constant monitoring and increased discipline potential); Cherry, *supra* note 183, at 991–93 (comparing the privacy rights of public sector employees to private sector employees in the United States and abroad).

226. Katsabian, *supra* note 19, at 247–49. Westin has offered a similar privacy policy already in the 1990s. However, unlike the suggestion made by this article, Westin's suggestion appears to be based on the good faith of the employer. *Cf.* Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values?*, 72 CHI.-KENT. L. REV. 271, 273 (1996) ("U.S. public generally prefers voluntary privacy policies to government regulation. Seventy-two percent of the public agreed in 1995 that 'if companies and industry associations adopt good voluntary privacy policies, that would be better

consider the specific characteristics and needs of both the employer and the teleworker and provide adjusted rules for the specific workplace.[227] It can also consider the specific characteristics and requirements of each role and employee and adjust the needed supervision to these elements in a genuinely proportional manner, taking into account the needs and rights of all relevant parties.

Such a policy should require that before the employer will be allowed to require its employees to install tracking apps in the home-office's technological devices, the employer and the employees' representatives *must* sit down together and agree on a privacy policy for teleworkers in the specific workplace, with adjustments for the specific roles and duties within it.[228] In other words, the prerogative of the employer to ask her workers to install tracking apps at the home-office should be contingent on the duty of the employer to generate a privacy policy at the workplace with the participation of employees' representatives.[229] If the employer does not create such a policy with the agreement and participation of employees' representatives, significant restrictions will be applied on the ability of the employer to install remote monitoring software.

The involvement of employees' representatives in this process is required to ensure that employees' right to privacy is being considered in a proportional manner along with the employers' interests and rights when applying monitoring apps.[230] Trade unions are, naturally, the most suitable

---

than government regulations, in this country.'"). For a critical analysis of Westin's argument, see generally Finkin, *supra* note 132.

227. *Id.* For further elaboration, see Einat Albin, Sectoral Disadvantage: The Case of Workers in the British Hospitality Sector, 274 (2010) (unpublished Ph.D. thesis, University of Oxford) (on file with the British Library, University of Oxford). Such a privacy policy will consider the unique character of the actual workplace—whether it is a public organization or a private one, a formal workplace or more "casual" one—as well as specific job descriptions, its hierarchical structure, and so forth.

228. *See* Katsabian, *supra* note 19, at 247–49.

229. This suggestion is a limited and modest version to restrict the employer's prerogatives when it comes to the employee's right to privacy in the telework case. There have been several much more radical and comprehensive suggestions to do so with regard to many other prerogatives of employers. *See* Gali Racabi, *Abolish the Employer Prerogative, Unleash Work Law*, 43 BERKELEY J. EMP. & LAB. L. 79, 79-80 (2022). *See generally* John D. Blackburn, *Restricted Employer Discharge Rights: A Changing Concept of Employment at Will*, 17 AM. BUS. L.J. 467 (1980) (discussing the case law history of at-will employment).

230. As scholars have clarified in the past, workers' representatives are the meaningful way to balance and even reduce the current power employers have in the U.S. (and also in global context). For further elaboration, see generally RICHARD B. FREEMAN & JAMES L. MEDOFF, WHAT DO UNIONS DO? (1984) at chapters 3–5. Note also, that some question union's motivation and ability to protect the right to privacy. *See, e.g.*, Westin, *supra* note 226, at 277 ("Labor unions have long protested when they saw coercive work monitoring used to drive workers to unrealistic and high-stress quotas. These protests have usually focused on unfair standards or inadequate compensation, not on the fact of supervisors watching or listening to workers at work. However, wholesale union opposition to work monitoring sometimes functions as an emotionally-charged weapon in the on-going power struggle between management and unions.").

entity to serve as the employees' representative in this process.[231] However, many workplaces in the United States do not have a formal trade union.[232] In that situation, the voices and interests of employees can be incorporated in other ways by using other forms of organizing workers, a discussion of which is beyond the scope of this Article.[233]

Various American and European scholars have made similar suggestions to more deeply involve employee representatives in decision-making processes regarding the right to privacy, mainly due to the shift to the digital workplace and the numerous new surveillance technologies that have accompanied it.[234] Bodie et al. argued that employees need a voice when it

231. *See* David Weil, *Individual Rights and Collective Agents: The Role of Old and New Workplace Institutions in the Regulation of Labor Markets*, *in* EMERGING LABOR MARKET INSTITUTIONS FOR THE TWENTY-FIRST CENTURY 13, 14 (Richard B. Freeman et al. eds., 2005); Davidov, PURPOSIVE APPROACH, *supra* note 213, at 238.

232. According to the U.S. Bureau of Labor Statistics, the union membership rate in 2020 was 10.8%. *See* Union Members Summary, U.S. BUREAU OF LAB. STAT. (Jan. 22, 2021, 10:00 AM), https://www.bls.gov/news.release/union2.nr0.htm [https://perma.cc/7ANM-W3FY].

233. For alternative forms of organization, *see* HARRY W. ARTHURS, FAIRNESS AT WORK: FEDERAL LABOUR STANDARD FOR THE 21ST CENTURY 131-33 (Gov't of Can., 2006) (proposing that in non-unionized workplaces a new "Workplace Consultative Committee" would be required); Alex J. Wood, *Networks of Injustice and Worker Mobilization at Walmart*, 46 INDUS. REL. J. 259, 269–71 (2015) (dealing with alternative forms of unionization of workers in the digital reality based on social media sites). *See also* Cynthia Estlund, *Rebuilding the Law of the Workplace in an Era of Self-Regulation*, 105 COLUM. L. REV. 319, 377–402 (2005) (discussing the various models of employee representation, particularly the hybrid model); CYNTHIA ESTLUND, REGOVERNING THE WORKPLACE: FROM SELF-REGULATION TO CO-REGULATION 170–212 (2010); Catherine L. Fisk, *Reimagining Collective Rights in the Workplace*, 4 U.C. IRVINE L. REV. 523 (2014) (presenting four alternative frameworks that empower workers to organize and take political action). One way to create a proportional balance between the employer and the employee with the assistance of employees' representatives, who are not organized in a formal trade union, is by having a semi-mandatory arrangement regarding the privacy policy that would be imposed on every workplace with more than a certain number of employees. The semi-mandatory arrangement would be written from the perspective of employees to guarantee strict protection of the right to privacy of the employee. This would create an incentive for employers to create a workplace-adjusted policy in collaboration with employee representatives. Otherwise, they would be exposed to legal action and forced to implement the relatively strict semi-mandatory arrangement. For further elaboration, see Katsabian, *supra* note 19, at 247–49; Guy Mundlak, *Information-Forcing and Cooperation-Inducing Rules: Rethinking the Building Blocks of Labor Law*, *in* LAW AND ECONOMICS AND THE LABOUR MARKET 55, 77–83 (Gerrit de Geest et al. eds., 1999).

234. *See, e.g.*, Sharon Block & Benjamin Sachs, *Clean Slate for Worker Power: Building a Just Economy and Democracy*, 29–37 (2020), https://lwp.law.harvard.edu/files/lwp/files/full_report_clean_slate_for_worker_power.pdf [https://perma.cc/D9PK-YKMG]; JULIET SCHOR, AFTER THE GIG: HOW THE SHARING ECONOMY GOT HIJACKED AND HOW TO WIN IT BACK 148–76 (2020). *See also* Work: Democratize, Decommodify, Remediate, https://democratizingwork.org [https://perma.cc/SR6J-4942] (last visited Aug. 27, 2020) (referring specifically to the need to involve workers in decisions workplace conduct as part of the learning process related to COVID-19); Ugo Pagallo, *The Group, the Private, and the Individual: A New Level of Data Protection*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGY 159, 184 (Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., 2017). For a skeptical analysis of trade unions' authenticity in their interest to represent the employees' right to privacy, see Guy Mundlak, *Human Rights and Labor Rights: Why Don't the Two Tracks Meet?*, 34 COMP. LAB. L. & POL'Y J. 217, 221 (2012). For a comparison regarding data protection in the workplace context of the EU, see Hendrickx, *supra* note 155, at 43.

comes to implementing practices of monitoring and decision-making based on employees' private data.[235] The involvement of employees in these processes is important not only to protect employees' rights but also to benefit the company because it encourages employees to feel more committed and loyal to the company.[236] In a similar manner, Rogers explained how workers' representatives are in the best position to consult on or bargain over employers' technological decisions, such as whether to deploy new monitoring devices at the workplace or use stored data to develop new algorithmic management systems. This is because the workers "are well-placed to understand both the costs and benefits of new technologies and may be able to respond to them in a more nuanced fashion than regulators."[237] It follows that the main role of lawmakers in this regard should be to empower workers and to enable them to more easily organize and be heard in the workplace.[238]

Finally, based on analyzing more than 1,000 company-level collective agreements concluded in Italy between 2015 and 2018, Dagnino and Armaroli similarly demonstrate the importance of involving workers' representatives in managerial decisions regarding employees' right to privacy.[239] According to the two, involving employees' representatives in such processes is crucial "not only to limit the quantity and fix the typologies of data collected and processed, against the risk of workers' surveillance, but also to co-decide over purposes and procedures of data processing, for the self-determination and concrete participation of workers".[240] Formal unions are already involved in the organization and regulation of telework in some countries.[241] International workers' organizations have particularly emphasized the importance of negotiating with trade unions on telework practices because of their implications for various workers' rights, including

235. Bodie et al., *supra* note 79, at 1032 (referring to the process of "people analytics").

236. *Id.* at 1035–37.

237. Rogers, *supra* note 79, at 580.

238. *Id.* at 581.

239. Emanuele Dagnino & Ilaria Armaroli, *A Seat at the Table: Negotiating Data Processing in the Workplace: A National Case Study and Comparative Insights*, 41 COMP. LAB. L. & POL'Y J. 173, 175–76 (2019).

240. *Id*.

241. An example of such involvement occurred in Canada in 1995. *See* Bryant, *supra* note 92 ("The Telecommunications Workers' Union (TWU) also reports that its collective agreement stipulates that electronic surveillance cannot be used as evidence for evaluation and disciplinary purposes."). However, Bryant later explained that there are only few cases in which trade unions were involved in such an arrangement. *Id. See also* EUROFOUND & INT'L LAB. OFF., *supra* note 24, at 48–49 (regarding the UK, Italy, Spain, Finland, Belgium, and the Netherlands, and dealing with the involvement of trade unions in regulating general issues regarding telework, beyond the question of privacy); Solon, *supra* note 94 (regarding teleworkers' efforts to unionize in Colombia to protect their right to privacy).

the right to privacy.[242] In some European countries, there are specific rules regarding the employer's ability to monitor teleworkers and the importance of basing the monitoring process on the employees' own documentation, or, at least, on collective agreement on this matter.[243] A general view of conditions in some European countries, beyond the specific case of telework, reveals how in Europe, collective representation has an important role to play when deciding on and applying a privacy policy in the workplace.[244] De Stefano similarly elaborates on the concrete importance of involving trade unions in today's workplace due to the increasing use of AI in employment and the tremendous power it provides employers over their employees.[245]

Because telework's hybrid nature blurs the private and professional even more than other privacy violations in digital reality, and due to monitoring technology's far-reaching capabilities, employee representatives should have an explicit place in the workplace's decision-making processes about the monitoring procedure. Employees' representatives can ensure that workers' rights are genuinely being considered and balanced against the employers' interests and prerogatives. They can also ensure that the right to privacy of third parties, especially minors related to the workers, are not being violated unjustifiably.

242. Armelle Seby, *Why Telework Needs Institutional Regulation and Collective Bargaining*, INDUSTRIALL GLOB. UNION (May 17, 2021), http://www.industriall-union.org/report-why-telework-needs-institutional-regulation-and-collective-bargaining [http://perma.cc/5TL7-GYKY].

243. Oscar Vargas et al., *Regulations to Address Work-Life Balance in Digital Flexible Working Arrangements*, EUROFOUND 29–30 (2020), https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef19046en.pdf [https://perma.cc/3SN6-KJR6] (describing such rules in Austria, Bulgaria, Croatia, Lithuania, Slovenia, and Spain).

244. Dagnino & Armaroli, *supra* note 239, at 177, 186–88 (comparing the United States and some European countries in this regard). *See also* Moore et al., Data Subjects, *Digital Surveillance, AI and the Future of Work*, EUR. PARLIAMENT 87 (2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf [https://perma.cc/2LHG-WP53] ("Precise identification of the seeming necessity for technological tracking must be infused with negotiation about what can be deemed proportional to workers' privacy and taking their wider interests seriously. Worker representative organisations must be involved in deciding necessity, proportionality and which workers' interests are at stake every time technological tracking processes are considered in every company and organization."). *Also see generally* Oscar Vargas Llave et al., *Telework and ICT-based Mobile Work: Flexible Working in the Digital Age*, EUROFOUND (2020), https://www.eurofound.europa.eu/publications/report/2020/telework-and-ict-based-mobile-work-flexible-working-in-the-digital-age [https://perma.cc/4FWM-AMFQ] (contending that the research on teleworking demonstrates how the use of digital technologies has enhanced the potential for remote workers to be intensively monitored from distance, and, therefore, works councils or other forms of employees' representative should have an important role to play in limiting the use of intrusive technologies for employees' monitoring).

245. De Stefano, *supra* note 79, at 46.

C. The Privacy by Design Approach

Since new technological programs are what enable employers to excessively intrude into the private life of teleworkers in the first place, the companies that generate these programs should also have legal duties.[246] This principle is consistent with the well-known basics of the corporate responsibility model—the idea that because corporations have a tremendous effect on an individual's rights and society's interests at large, they should follow several basic principles in their ongoing activity, whether voluntarily or involuntarily, to ensure human rights and common goods protection.[247] Scholars have also made similar suggestions—called "algorithmic accountability"—regarding AI technology and the responsibility of AI companies and programmers to ensure that their products do not violate human rights, including the right to privacy.[248] The European Union recently published its proposed "Artificial Intelligence Act," aimed at regulating the implications of AI for human rights already from the designing process.[249] Such approaches can ensure that the right to privacy is taken into consideration by all parties that can influence this right.[250] The most relevant suitable approach to ensure that products—and the companies that create them—will not intrude into workers' privacy more than necessary is the privacy by design approach.

---

246. *See supra* notes 195–198 and accompanying text.

247. *See generally* MICHAEL BLOWFIELD & ALAN MURRAY, CORPORATE RESPONSIBILITY (2014) (showing, by using several case studies, how corporate responsibility became increasingly central to business and their social and economic role in the twenty-first century); SIMON ZADEK, THE PATH TO CORPORATE RESPONSIBILITY: CORPORATE ETHICS AND CORPORATE GOVERNANCE 159 (2007) (focusing on the way Nike embraced the principles of corporate responsibility); NEIL W. CHAMBERLAIN, THE LIMITS OF CORPORATE RESPONSIBILITY (1973) (focusing on the implications of corporate responsibility for various parties and aspects—such as employees, shareholders, the environment, the education system, the local community, national policy, and international relations); Kenneth E. Goodpaster, *The Concept of Corporate Responsibility*, 2 J. BUS. ETHICS 1 (1983) (developing a systematic approach to the field of business ethics by introducing the 'principle of moral projection' as a device for relating ethics to corporate policy).

248. *See generally* Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54 (2019) (discussing the relationship of civil rights to algorithmic accountability).

249. For a broad overview of the implications of this proposed Act on workers' rights, see generally Mirian Kullmann and Aude Cefaliello, *The Draft Artificial Intelligence Act (AI Act): Offering False Security to Undermine Fundamental Workers' Rights* (Dec. 23, 2021), http://dx.doi.org/10.2139/ssrn.3993100 [https://perma.cc/SU9V-SLMT]; Jeremias Adams-Prassl, *Regulating Algorithms at Work: Lessons for a 'European Approach to Artificial Intelligence'*, EUR. LAB. L. J. (2022), https://journals.sagepub.com/doi/pdf/10.1177/20319525211062558 [https://perma.cc/F2FD-GN6Q].

250. *Cf.* Christoph Lutz & Aurelia Tamò, *RoboCode-Ethicists: Privacy-Friendly Robots, an Ethical Responsibility of Engineers?*, PROC. OF THE ACM WEB SCI. CONF. 3.2, 3.3 (June 2015), https://dl.acm.org/doi/10.1145/2786451.2786465 [https://perma.cc/XW9T-H6P5] (dealing with a similar dilemma with regard to formation of robots and privacy); POSTER, *supra* note 197 (dealing with a similar dilemma with regard to monitoring in call centers).

The privacy by design approach is a paradigm generated to provide greater privacy protection.[251] It is a systematic, proactive method that requires privacy to be taken into consideration throughout a product's lifetime, starting with the initial stage of product development and ending with the final stage of its service life.[252] The privacy by design approach was initiated in the 1990s against the backdrop of the development of the information society and the numerous new challenges to the right to privacy it was creating.[253] Since the passive protection of privacy could not effectively deal with the rapidly increasing new threats to privacy, a new privacy-protection approach was required—one that was more proactive and comprehensive.[254] The privacy by design approach emphasizes that the future of privacy cannot be assured by only compliance with regulatory frameworks; rather, privacy must become an organization's ongoing default mode of operation.[255] This new approach has been embraced by several entities, including within the General Data Protection Regulation (GDPR) in European countries.[256] In 2012, the US Federal Trade Commission (FTC) offered its interpretation of the privacy by design approach, focusing mainly on three core principles: privacy by design, simplified choice, and transparency.[257]The FTC called the Congress "to enact comprehensive privacy legislation that draws on the ideas in the FTC's framework" and as a result, this approach applies only on a voluntary or self-regulatory basis.[258]

---

251. Fei Bu et al., *"Privacy by Design" Implementation: Information System Engineers' Perspective*, 53 INT'L J. INFO. MGMT. 2 (2020), https://www.sciencedirect.com/science/article/pii/S0268401219308606 [https://perma.cc/H8GA-QZ2J]; *see also* Peter Hustinx, *Privacy by Design: Delivering the Promises*, 3 IDENTITY IN THE INFO. SOC'Y 253, 253–54 (2010).

252. The approach of privacy by design was initiated in Canada; however, both the EU and the United States have embraced some of its core elements. *See generally* ANN CAVOUKIAN, PRIVACY BY DESIGN IN LAW, POLICY AND PRACTICE, A WHITE PAPER FOR REGULATORS, DECISION-MAKERS AND POLICY-MAKERS 26 (2011) [hereinafter Cavoukian, *White Paper*]; Ann Cavoukian, *Privacy By Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices* 1, 4 (2009), https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf [https://perma.cc/ZY4S-GTS3] [hereinafter Cavoukian, *7 Foundational Principles*]; Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1410–11 (2011).

253. Bu et al., *supra* note 251.

254. *Id.*

255. Ann Cavoukian et al., *Remote Home Health Care Technologies: How to Ensure Privacy? Build It*, *in* PRIVACY BY DESIGN 363, 369 (2010), https://link.springer.com/content/pdf/10.1007/s12394-010-0054-y.pdf [https://perma.cc/ZY4S-GTS3].

256. For further elaboration, see GDPR, *Privacy by Design* (2018), https://gdpr-info.eu/issues/privacy-by-design [https://perma.cc/9QXY-WCW8].

257. Edith Ramirez, Comm'r, Remarks at the Privacy by Design Conference 1 (Jun. 13, 2012) (transcript available at https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf [https://perma.cc/9KCX-ZG77]).

258. *Id.*

The privacy by design approach includes several basic principles that all actors in the process of generating a product must follow to ensure that a product will not violate the right to privacy.[259] These principles are: (1) proactivity rather than reactivity: anticipating and preventing privacy-invasive events before they happen; (2) privacy as the default: ensuring that the personal data of the individual is automatically protected in any given technological system as the *default*, even if the individual does nothing to actively protect her privacy; (3) embodiment of privacy within the design process, with privacy integral to the system as an essential component of the product; (4) functionality: a product can and should be both functional and privacy-protective; (5) end-to-end life cycle protection: embedding privacy into the system before the first element of information is collected and extending it throughout the life cycle of the data involved; (6) visibility and transparency: making the product's components and functions visible and transparent to users and providers alike; and finally, (7) respect for users' privacy: ensuring that architects and operators keep privacy defaults, for instance, by providing an appropriate notice for an optional privacy violation or empowering user-friendly options.[260]

The idea of privacy by design is usually associated with subjects such as health systems, cloud computing, the Internet of Things (IoT), biometric encryption, and big data.[261] In recent years, however, due to the increasing

259. Seda Gürses et al., *Engineering Privacy by Design*, 14 COMPUTS., PRIV. & DATA PROT. 25, 27 (2011); Cavoukian, *7 Foundational Principles*, *supra* note 252, at 5. Over the years, the OECD has expanded these basic principles to eight basic principles: (1) Collection Limitation Principle—There should be limits to the collection of personal data and the collection has to be made lawfully by using fair means with the notice and consent of the data subject; (2) Data Quality Principle (Personal)—The collected data has to be relevant to the purposes for which it is used, and, to the extent necessary for those purposes (a proportionality principle); (3) Purpose Specification Principle—The purposes for which personal data are collected should be specified at the time of data collection at the latest; (4) Use Limitation Principle—Personal data should not be disclosed or made available for use for any other purpose other than those that were mentioned in the "Purpose Specification Principle" (with some exceptions); (5) Security Safeguards Principle—Personal data should be protected by reasonable security safeguards; (6) Openness Principle—a general policy of openness about developments, practices and policies with respect to personal data, should be developed; (7) Individual Participation Principle—An individual should have the right to receive from a data controller confirmation of whether or not the data controller has data relating to her, to get this information within a reasonable time at a charge, if any, that is not excessive, and to receive a reasoned letter in a case if denial on which an individual has a right to appeal; (8) Accountability Principle—A data controller should be accountable for complying with measures which give effect to the principles stated above. For further elaboration on these principles, see Cavoukian et al., *supra* note 255, at 370–73.

260. *See* Gürses et al., *supra* note 259; Cavoukian et al., *supra* note 255, at 370–73.

261. Bu et al., *supra* note 251, at 2–3 (providing a general overview of the various ways privacy by design is utilized). *See also* Ann Cavoukian, *Privacy in the Clouds*, 1 IDENTITY IN THE INFO. SOC'Y, 1, 89 (2008) (discussing cloud computing's relationship to privacy by design); Ann Cavoukian et al., *Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment*, 29 REV. POL'Y RSCH. 37, 40–41 (2012) (analyzing biometrics and privacy by design); Cavoukian et al., *supra* note 255, at 373-75 (looking at health care systems and privacy by design); Ann Cavoukian et al., *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices*, 3 IDENTITY IN THE INFO. SOC'Y 405, 406–08 (2010) (discussing the intersection between business and

use of intrusive monitoring tools in the workplace, the privacy by design approach has gradually been more used in the workplace context.[262] As part of this trend, when cybersecurity programs that seek to eliminate threats from within the workplace or by outside online invaders are developed and used, it is important that the privacy by design approach be followed and that the monitoring program ensure both functionality (i.e., protection against cyber risks) and employees' privacy.[263]

This is particularly true when the work is being done from home, in the private sphere of the employee, where the employee's private information and surroundings, including third parties, are exposed to the risk of privacy violations. However, as I have shown, it is precisely in the home-office that employers use the most intrusive monitoring tools to ensure that the teleworker actually works from home. It is quite clear that the right to privacy was not taken into consideration *at all* throughout the engineering and production processes of these tools. These programs' marketing websites make this obvious.[264] The only interests that the monitoring companies considered were those that coincided with their own interests: the employer's interests. It is no wonder, then, that these monitoring programs involve massive intrusions into the employee's private sphere beyond what is necessary. This is especially true of programs that are installed on the employee's private devices without notice to the employee.[265] It is also the case, however, for the "ordinary" monitoring programs available in the market today.[266]

The leading principle in this context should therefore be that along with the obvious need of the employer to verify that its workers actually work from a distance and that there are no security risks, the monitoring program must respect workers' right to privacy and follow the privacy by design approach. When designing a program that monitors from a distance, the engineers and producers of these programs must plan and include in the program default that will ensure employees' and third parties' privacy. Following this basic concept will ensure that the monitoring program follows

---

privacy by design); Abhik Chaudhuri, *The Proactive and Preventive Privacy (3P) Framework for IoT Privacy by Design*, 57 EDP AUDIT, CONTROL & SEC. 1, 6–8 (2018) (analyzing the "Internet of Things" (IoT) and how privacy by design impacts it); Eric Everson, *Privacy by Design: Taking Ctrl of Big Data*, 65 CLEVELAND ST. L. REV. 27, 28–30 (2016) (looking at big data and its relationship to privacy by design).

262. *See, e.g.*, Paul Wood, *Socio-Technical Security: User Behaviour, Profiling and Modelling and Privacy by Design*, *in* CHALLENGES IN THE IOT AND SMART ENV'TS. ADVANCED SCIS. AND TECHS. FOR SEC. APPLICATIONS 75 (R. Montasari, H. Jahankhani & Al-Khateeb H. eds., 2021).

263. *Id.*; see also description of fourth criterion of the privacy-by-design approach *supra* notes 259–260 and accompanying text.

264. *See, e.g.*, the monitoring programs websites that were mentioned above. (Hubstaff, Time Doctor, Teramind, Pragli).

265. *See* Lynn, *supra* note 95.

266. *See* discussion *infra* Part II.A.1 on the monitoring programs Hubstaff, Time Doctor, Teramind, Pragli.

criteria one through three and five in the privacy by design approach discussed above. It will ensure a proactive approach to protect privacy and set privacy as the default of the program. Similarly, it will embody privacy in the very initial stage of designing a product, and all along the way of generating and producing it. Tech companies should, naturally, do so in a way that ensures both functionality and privacy protection in accordance with criterion four: employers will be able to reduce security risks and ensure that their workers actually work, but without eliminating employees' and others' right to privacy. Finally, tech companies should also include features that increase the visibility and transparency of what is being monitored and how and do so in a way that is accessible by and clear to the average user, i.e., to the average employer and employee. This last element will follow criteria six and seven in the privacy by design approach.

As was described in Part III.A, these requirements can be achieved in various ways. One possibility is the creation of a system in which the employee reports in detail on her activity during her working day or when a reporting message pops up on the employee's screen.[267] Another way can be that the program will only document distinct private web pages that the employee has been visiting for longer than fifteen minutes per day, for instance, without exposing the content of the page. The program could also delete the accumulated data at the end of every day. There are numerous ways to both ensure cybersecurity and the productivity of the worker and protect her right to privacy. By applying the principles of privacy by design to the program, companies will ensure that they take the right to privacy into consideration, which will result in a better holistic solution model to resolve the home-office privacy dilemma.

This is true for both the explicit monitoring-from-distance programs[268] and the supposedly neutral programs that provide the employer with private information on the employee or on third parties (mainly, the employee's surroundings).[269] It is true of the teleworker's right to privacy and all the more, the right to privacy of third parties, who are not part of the workplace

267. See the explanation provided in *supra* note 222.

268. For example, see in-depth discussion of Hubstaff, Time Doctor, Teramind, Pragli, and InterGuard *infra* Part II.A.1.

269. Microsoft 365 or Zoom are helpful examples of this, as discussed in depth *infra* Part II.A.1. The same is true, of course, with regard to the information these programs collect on their clients, regardless of the workplace context. For further elaboration of this issue, see Fry, *supra* note 122 ("On March 26th, a journalist for Motherboard revealed that Zoom was using software that shared customers' data with Facebook."). *See also Zoom Privacy Statement* (Dec. 15, 2021), https://explore.zoom.us/en/privacy/ [https://perma.cc/43JN-LDHA] (according to which Zoom collects a laundry list of data on its clients, including their user names, physical address, email address, phone numbers, job information, Facebook profile information, computer or phone specs, IP address, and any other information that the costumer uploads, provides, or creates while using the service. Zoom clarified that recorded meeting can provide the company with the collected information in connection with and through such recordings, including personal data).

context and are not aware of, much less agreeable to, their privacy being violated. Applying the privacy by design approach in all these cases can ensure better protection of privacy for all relevant parties, a priori and not in retrospect, without harming the employer's interests.

IV. CONCLUSIONS

The COVID-19 pandemic has expedited numerous technological changes in the labor market and in doing so provided an intense glimpse into the workplace of the future and the new challenges it will bring. Among other things, it has illuminated how telework is about to become an integral part of the future workplace. It has also powerfully shown the vast implications telework will have for the employee's rights to privacy.

As this Article shows, the phenomenon of telework has generated a new hybrid location, the home-office, which combines the private sphere of the employee with her professional life. Due to its hybrid private-professional nature, the home-office has triggered violations of the employee's right to privacy and raised questions about what the employer can supervise. It has also exposed how the current privacy difficulty involves third parties as both privacy violators and victims. The telework case continues the current trend of the employee's and others' right to privacy being limited in the new digital reality by the new surveillance technologies it has brought with it.

The telework example thus requires us to pause and rethink current policies and emphasizes how much change is required. It has exemplified how the required modification in the workplace context must be made in a proportional and adaptable manner, together with employees' representatives, and be sensitive to the specific power dynamic in workplaces and to nonroutine events. Telework and the phenomenon of the hybrid home-office have also clarified that the required policy changes cannot focus on the workplace domain only. They must tackle other domains relevant to the issue at stake, particularly the tech industry. Genuine protection of labor rights in the future digitalized workplace must explicitly and fully involve employees' representatives in the workplace's daily routine and the employer's managerial decisions. We should also broaden the scope of labor rights protection and involve additional actors – in this case, tech companies – in the regulatory process of labor rights. In other words, the telework case has clarified the importance of employees' representation to the broad scope of violations of employees' rights in today's world and technology's connection with broader societal and economic structures.