Bring Your Own Device — Now Hand It Over! Rescuing Workers' Privacy During Data Searches

VIRGINIA MANTOUVALOU & MICHAEL VEALE*

Technological advancements pose serious threats to workers' privacy. This article focuses on practices that greatly blur the line between workers' private life and life at work, such as the practices of "bring your own device," and linking cloud storage to personal and work devices. The first sees workers allowed to use personal devices for work-related activities, potentially for several employers. The second sees workers using online storage for personal and professional reasons, linking this storage to personal and work devices. Such practices can be useful for workers. However, they also present challenges for workers' privacy, particularly when other legal frameworks are implicated. Employers may have legitimate reasons and a legal basis to request access to, control, and search of workers' devices on the basis of, *inter alia*, data protection, freedom of information, and civil procedural rules. These rules may promote other legitimate goals. However, when individuals do not separate their private and professional activities cleanly within or across devices in a way that can be searched, the legal regimes in question can pose threats to privacy. These regimes may require analysis of unseparated material through accessing data and devices. This article examines this trend with a primary focus on United Kingdom and European law. We propose that workers' right to private life should be understood as a right to supported separation of work and private contexts and a right to control the process of a search of data and devices.

Keywords: Privacy, Worker Privacy, BYOD, cloud storage, reasonable expectation, human rights

---

* Virginia Mantouvalou, Faculty of Laws, University College London; Michael Veale, Faculty of Laws, University College London. This article has benefitted from research assistance by Jeevan Shemar, and input from Einat Albin, Hugh Collins, Nicola Countouris, Michael Ford, Jake Goldenfein, Marta Otto, Karen Scott, Yuval Shany, Hannah Willcocks, two anonymous reviewers, the "Privacy@Work in an Era of New Technologies" conference, the London Labour Law Discussion Group, the Durham Human Rights and Public Law Centre (with particular thanks to Ben Yong and Natalie Sedacca), and a UCL Faculty of Laws staff research seminar. Michael Veale was supported by the *Fondation Botnar* and the UKRI Trustworthy Autonomous Systems Hub (EP/V00784X/1).

I. INTRODUCTION

TECHNOLOGICAL ADVANCEMENTS HAVE RECONFIGURED THE HOME and the workplace. This reconfiguration has led to serious threats to workers' privacy. In this article, we focus on practices that greatly blur the line between workers' private life and life at work, such as the practice of "bring your own device" (BYOD) and the practice of linking work and private devices to cloud storage. The first practice, BYOD, sees workers allowed to use their personal devices for work-related activities, which can be convenient, familiar, and supportive of flexible working, potentially for several employers. The second practice involves workers using online storage tools, such as OneDrive (Microsoft) or iCloud (Apple), using either personal or employers' professional plans, to store personal information from their devices, and connect this storage to work devices. Photos, private messages, and other personal items that may even involve intimate aspects of people's personal life intermingle in a space that is neither purely personal nor purely professional. Individuals may save time by using these tools and engaging in these practices, and may find it simple and convenient, but they are also presented with a new problem: a real blurring of the boundaries of personal and professional life. The practices that are examined here are not the only instances where technology creates threats to workers' privacy or digital rights more broadly, of course (Aloisi & De Stefano, 2022; Bogg et al., 2024, Chapters 13–14; Ekbia

https://digitalcommons.osgoode.yorku.ca/cllpj/vol45/iss3/4
DOI: 10.60082/2819-2567.1065

& Nardi, 2017; Levy, 2023; Mantouvalou, 2019). Yet the practices presented in this article pose a distinct challenge to workers' privacy.

Privacy, data protection, and computer misuse law may provide protective answers if an employer or their agent was opportunistically rummaging through a worker's files for an illegitimate purpose, such as gossip or retribution. Yet, under other regimes that may purport to protect individual rights, employers may have legitimate reasons, a legal basis, and even an obligation to request access to control and monitor workers' devices. Such regimes include freedom of information (FOI) law, laws concerning cybersecurity, specific sectoral regimes, or general civil procedural rules during a dispute. Some of these laws, such as data protection law, are even the same regimes that workers might hope to employ in order to protect their rights. All these regimes (and more that we examine in Section III) may oblige employers to bring workers' data and devices within the scope of a search for information. This places workers in a difficult position. To understand their options, they may have to assess the nature of the legal obligation on the employer (or themselves), likely without independent counsel and perhaps without union representation, and within the power imbalance characterised by the employment relationship. Consequently, it can be particularly difficult for workers to turn down requests by employers to access their devices.

In the past, when a request to access materials was triggered, a worker may have been able to simply hand documents from a filing cabinet in their office over to their employer without it troubling them particularly. This is no longer the case. The danger now is that employers can dominate workers' lives not only because of the economic inequality inherent in the employment relationship but also because of the informational infrastructures in which their employment is enmeshed. A couple of problems emerge.

First, individuals do not separate their activities cleanly within or across devices in line with a personal or professional divide. It is common — even encouraged in some workplaces — to use personal messaging apps in professional environments. Studies in human–computer interaction have well-documented that people may try, but struggle, to keep professional and personal "communication places" separate in contemporary app ecosystems (Griggio et al., 2022; Nouwens et al., 2017). It has even become common for some employers to request that workers stop trying to separate personal and professional life, instructing them instead to "bring their whole self to work" (Eustace, 2025; Paul, 2022; Robbins, 2018).

Second, unorganised data, such as text messages, is not always easily searchable, particularly considering that the scope of and tests within relevant data access regimes can be extremely unclear (Dalla Corte, 2019; Purtova, 2018).

Assessing this scope often requires analysis of unseparated material. The easiest way for employers is to have direct access to the device. This is also the most invasive way, and the threat to workers' privacy is obvious. This threat is greater for precarious workers, such as workers employed through agencies or zero-hour contracts. These precarious workers may work for several employers, may not know their true employment status with any particular one of them, may be less likely to have worker-issued devices to aid separation of context, and lack bargaining power to resist unreasonable or unlawful requests.

We proceed by explaining what we mean by referring to the blurred private and professional context in light of information technologies in Section II, which aims at illustrating the extent of the challenge. In Section III, we turn to the law and we present some examples of legal regimes that may promote legitimate and even worker-protective goals, but that also provide a legitimate basis for accessing workers' storage and private devices — practices that particularly concern us in this article. Our focus is on United Kingdom (UK) and European Union (EU) law. Section IV considers some of the forms that the search typically takes and the privacy concerns that each modality poses. Having discussed these, in Section V, we explain which principles should govern these practices, drawing on case law on the right to private life as protected in the European Convention on Human Rights (ECHR). We suggest that the right to private life in this context should be understood as a right to supported separation of work and private contexts, as well as a right to control the process of a search of data or devices. Such protections should be explicitly added to legal regimes, and we suggest concrete ways to do this, rather than leaving both employers and employees in the dark about what should happen when a broad, valid legal basis for a search is established.

II. DEVICES AND STORAGE AT WORK

A few decades ago, there was typically a clear, difficult-to-blur division between professional and personal material. The work/life informational distinction was relatively sharp, and preserving it was straightforward in most cases.

Such separation even persisted when employers' informational infrastructures entered private spheres. Early "tele-workers" were often provided with their own phone-lines when working from home, and they organised their activities to preserve such separation (Dutton, 1999; Ellison, 2004). This now-antiquated term was associated with stationary computers, fax machines, and so on provided by the employer, not the mobile, cloud–based computing we see today, either on

personal devices or on devices functionally identical to widely owned personal counterparts (Messenger & Gschwind, 2016). The earliest generations of electronically mediated telework came before the overwhelming societal adoption of computing for leisure, social, and personal communication, leading workers to primarily use these devices for work. These devices, and any information on them, could be recovered at the termination of employment. Yet, over the years, separation has become less practicable. The growth of "personal computing" saw individuals adopt, in their homes, devices previously only found at work (Nooney, 2023), which created the technical potential for this blurring. "Personal" devices became familiar, convenient, even intimate.

There are several routes through which individuals might find their personal devices entangled with content related to their workplace. Some employers authorise or even require workers to "bring [their] own devices" (BYOD), a practice that can be positive for reasons such as familiarity and convenience (and low cost for employers) but also raises concerns including IT security, workers' privacy, and working time (Blair, 2018; Jimenez & Jahankhani, 2020; Kahvedžić, 2021; Stewart, 2019; Wang et al., 2014). Workers may also use their own devices without official permission. These are commonly called "shadow IT" systems (Silic & Back, 2014), unauthorised by IT divisions, and often include personal, consumer devices brought into work (Kopper & Westner, 2016). Even where they are not officially permitted, demands of the job, of colleagues, and of managers mean their use is not always to be frowned upon or their use actively discouraged. Indeed, some commentators note that they bring significant potential for workplace innovation and efficiency (Harris et al., 2012; Silic & Back, 2014). For example, WhatsApp is highly popular in its unofficial usage across the world in workplaces such as hospitals, schools, and governments (Durrant et al., 2022; Gulacti et al., 2016; Opperman & Janse van Vuuren, 2018; Varanasi et al., 2021).

On top of the combination of work and private information is the changing accessibility of such information to the employer. In the past, materials accessed and stored on someone's home computer were often not well connected to their work network and could not be accessed by their employer without the worker's co-operation. Yet, in more recent years, sociotechnical developments have blurred this line. The use of cloud storage is a core example here. Employers often provide high-capacity cloud storage for their workers, for example, through Google Cloud accounts. These storage systems can often be synced onto personal devices. They may not stay compartmentalised within such devices: such tools often also synchronise with just a few clicks the contents of folders such as Desktop or

Documents, which are not specifically labelled for work (Microsoft, n.d.). This places private files and folders of individuals onto a server that can technically be accessed by the employer without the worker's awareness. The reverse is also possible: individuals do, for personal convenience or to achieve workplace tasks using familiar tools, add their personal cloud storage accounts to devices owned by the employer, which then places individuals' personal files onto employers' servers (Haag, 2015). They may specifically use these for work purposes too: in 2016, 83% of 500 IT decision-makers surveyed in the UK, France, Spain. and Germany reported that their employees used free, unregulated cloud storage services with personal accounts, such as Dropbox or Google Drive to store company documents (NTT Communications, 2016). A similar issue occurs when workers use tools that synchronise end-to-end encrypted messengers, such as Signal or WhatsApp, to work devices (e.g., to use the bigger keyboard), as in the process, these tools store copies of received messages that were previously only on their phone.[1]

Making things even more complicated, some employers incentivise or even require their workers to connect their professional devices to personal cloud services (Schiffer, 2021). Take Jacob Preston, who was reportedly told by his manager when he started working at Apple that he needed to link his personal Apple ID and work account (Schiffer, 2021). We found it a strange request, knowing that his Apple ID was connected to his personal data, such as his messages. However — and in the context of the power imbalance between employer and employee — he linked his accounts. When he resigned a few years later, he was asked to return his work laptop without wiping the computer's hard drive, which due to this linkage contained, as he explained, highly personal information. Despite his refusal, he was not permitted to completely wipe it, leaving that data in the hands of his former employer.

A related risk comes from installing employers' cybersecurity monitoring systems, which are often prerequisites to connecting to an employer's network from a personal device. Such tools as *Microsoft Defender Endpoint* or *Crowdstrike Falcon* can be set up to be highly invasive, scanning content, application usage, network usage, and even keystrokes, disclosing significant information about individuals (Toch et al., 2018). Companies take more control over devices, even those that they do not own, by enrolling them in mobile device management (MDM) systems, such as those provided by Google (*Endpoint*) and Apple

1. For example, one of the only ways to retrieve and export Signal messages from a phone is to take a copy synchronised from a computer using a tool such as sigtop. See the source code for this at https://github.com/tbvdm/sigtop

(*Platform Deployment*), which give employers some control over workers' devices and the data on it (Yamin & Katt, 2019). This has been heightened by concerns around ransomware, particularly in organisations, such as schools, which may not be able to afford work mobile devices. As a result, a range of workplace monitoring systems have become popular in an attempt to ensure that malware cannot enter the network and sensitive data cannot leave it.

Even if both the employer and the employee think that a separation of professional and private information in the workplace would be best, the contemporary technological landscape does not easily facilitate this. The diligence required to separate data in an always-online world can be enormous, and time-poor workers have limited bandwidth to navigate this given both the pace of contemporary life and the lack of digital literacy (and organisational transparency) as to who data is transferred to, when and how. This can be best understood through the lens of the extensive literature on the failures of privacy self-management and individualistic control of data, as the logistics of data management in the workplace are no different, and potentially even more daunting, than the management of data in personal settings (Barocas & Nissenbaum, 2014; Bietti, 2020).

Individuals' awareness of monitoring or potential monitoring undertaken by their employers is low (Rosengren & Ottosson, 2016, p. 189). So, it follows, is any ability to navigate and manage the private–professional divide amidst these technologies. Considering these features, it is obvious that work and personal life are blurred in ways that could not have been envisaged in the past when work materials would be in people's office at work, and private materials would be at home, and the mechanics by which they are transferred were visible and predictable. Today both work and private materials are accessible through work and private devices. Some companies sell "solutions" designed to try to restore this separation by creating a set of apps — for example, a separate corporate version of WhatsApp that automatically backs up to company servers (Microsoft, 2023). However, this is only within reach of large, high-capacity firms, particularly in industries with significant compliance obligations, and furthermore relies on the diligence of workers to re-establish the separation within their devices.[2] If this separation fails, information that is private, such as people's personal photos and communications, is at risk of being accessed or claimed by employers. This is particularly the case when legal grounds to access information that falls within these blurred boundaries are established. The section that follows turns to some of these legal grounds.

2. For example, the *ex ante* separation obligations we detail in s 4.1.

III. LEGAL BASES TO REQUEST ACCESS

What makes this blurring of the lines more difficult to navigate is that employers often have legitimate reasons to request access to devices or storage. This may not only be for reasons of economic efficiency, say as a way to measure workers' productivity, which is often invoked as a basis to restrict workers' rights. Requests to access private devices may also be based on the rights of third parties grounded in legislation. Many legal regimes provide for access to a variety of types of information that may be held on workers' devices. We provide a non-exhaustive overview of some of these regimes below. It is important to explain that these regimes may at times be effective in serving worker-protective and other legitimate goals. However, the overarching point for the purposes of our argument is that they sometimes provide legitimate reasons and a legal basis to access employees' data and devices. The challenges we outline in this article are real, and cannot be written off as artefacts of unjust regimes.

A. DATA PROTECTION

Data protection laws around the world offer individual data subjects the right of access to personal data, namely information that relates to them and that renders them identified or identifiable.[3] In both the EU and the UK (as well as the majority of the 137 countries around the world with some form of data protection or privacy law and typically similar drafting) (United Nations Conference on Trade and Development, 2023), the scope of personal data is wide. It extends into the parts of the texts or emails concerning a person, including opinions about that person.[4] Personal data includes large amounts of free text, which has increasingly entered the scope of the law as communication has digitised. Requests can be broad. Depending on the nature of the request, employers may then have a duty to go through documents, emails, or potentially even messages sent between two colleagues on a messenger such as WhatsApp.

Employers only have a duty to provide data if they are the relevant data controller. However, this concept is understood broadly, and the Information Commissioner's Office in the UK notes that "if you [a company] do permit staff to hold personal data on their own devices, they may be processing that data on

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, articles 4(1), 15 (hereafter GDPR).
4. Case C434/16 Nowak ECLI:EU:C:2017:994, para 34.

your behalf," which will lead to a determination of controllership (Information Commissioner's Office, 2023). In practice, as the scope of personal data is wide, it is becoming practically impossible to forbid staff from holding personal data on their own devices, as such data could even consist of a message between two colleagues about a third in a work context. If an individual requests this type of information, an employer's duty will quickly extend to messages in these spaces. Non-staff members, such as non-executive directors or trustees, are also likely to be in scope, and these individuals rarely have work devices due to their less active engagement (Tan & Leech, 2021). Of consideration is also whether an employee or director is acting in a "rogue" manner, or whether they are doing so on behalf of their employer.[5]

Courts examining such subject access requests have found that the employer's duty to supply this information is subject to a test of proportionality: the employer does not have to "leave no stone unturned."[6] Yet this search effort can still be costly, with one case regarding emails in a dispute at the University of Oxford incurring search costs of over £116,000.[7] The process of the search for relevant materials can also be intrusive of personal folders and documents. While there are grounds to refuse to provide data in an access request, such as in cases where providing the data might interfere with rights of others, such as privacy or intellectual property, these only apply after the search has been carried out. For our purposes, the concern is the *process of the search itself* by the employer, rather than the outcome of the request. While the data subject may be successfully prevented by the data protection regime from receiving private information of another, the employer may still have had to examine potentially sensitive information in order to make that determination. This search is itself an interference with privacy.

B. FREEDOM OF INFORMATION

Freedom of information (FOI, sometimes FOIA) laws also exist around the world in different forms. Public sector workers and other individuals holding information on behalf of an authority with FOI duties can find their correspondence subject to these rules.[8] While some public sector organisations

5. *Harrison v Cameron* [2024] EWHC 1377 (KB) [84].
6. *Ittihadieh v 5-11 Cheyne Gardens RTM Company LTD & Ors*; *Deer v Oxford University* [2017] EWCA Civ 121, para 103.
7. *ibid.*, para 26.
8. *King's College, Cambridge v IC* [2013] UKFTT EA/2012/0049 (GRC); *University of Newcastle v IC and BUAV* [2011] UKUT 185 (AAC).

operate tight operational security, the long tail of entities within scope, such as tiny parish councils, have next-to-no IT capacity, or chance of being issued work devices. University workers, in jurisdictions including in the UK, New Zealand, and some US states, can also find their correspondence at risk of being requested, which has long drawn criticism in relation to impact upon academic freedom, particularly concerning political or corporate retaliation for research (Woodbury, 1994).

This tension has become further apparent as FOI requests have hit up against government business carried out through "non-corporate communication channels" such as WhatsApp or Signal, particularly with "disappearing messages" enabled, a form of ephemeral messaging where both senders' and receivers' records are erased after being viewed or after a preset amount of time has elapsed.[9] Attempts to evade FOI law using private email accounts have been happening for many years, leading to increased clarity from regulators that there are conditions under which such private channels can fall within the scope of the law (Cook, 2011).[10]

A more arcane ancestor of FOI law created a BYOD tension in 2019 in the UK, as the Member of Parliament Dominic Grieve sought to use the broad parliamentary power to call for papers, taking the form of a "humble address to the Crown," in order to force Ministers to produce

> [(…] WhatsApp, Telegram, Signal, Facebook messenger, private email accounts both encrypted and unencrypted, text messaging and iMessage and the use of both official and personal mobile phones) to, from or within the present administration, since 23 July 2019 relating to the prorogation of Parliament […]

sent by listed individuals including the then-Prime Minister's Chief of Staff, Dominic Cummings.[11] The government resisted this part of the address on privacy grounds, stating that such use "goes far beyond any reasonable right of Parliament under this procedure," that the "individuals have no right of reply, and the procedure used fails to afford them any of the protections that would properly be in place [and] offends against basic principles of fairness and the Civil

9. This functionality auto-deletes messages from both sender and recipient within a certain number of days. Some UK Government services have disappearing messages after 24 hours enabled by default; see *R (All the Citizens & Anor) v Secretary of State for Digital, Culture, Media and Sport & Ors* [2022] EWHC 960 (Admin) [29], [34]. In the US context, see generally Stewart (2019).
10. Information Commissioner's Office, *Decision Notice IC-40467-C7K2* (31 March 2022), para 51.
11. *Hansard*. (2019, September, 9). House of Commons Debate (664), col. 522. On the procedure, see Erskine May: Parliamentary Practice (25th ed., 2019) para 7.31.

Service duty of care towards its employees."[12] In the end, it seems that this saga fell by the wayside as the relevant Supreme Court case took centre stage.[13] That was not quite the end, however — a nearly identically worded FOI Act request relating to Cummings was upheld by the Information Commissioner, who found that the Cabinet Office should have undertaken searches of Cummings' personal devices — but, by then, he had left the government.[14]

C. PROCEDURE

Private messages can become important evidence in legal proceedings, and are often at stake in employment disputes. Courts and tribunals regularly examine private messages, such as those on WhatsApp, in cases involving harassment at work and disciplinary action.[15]

Civil procedure disclosure rules provide a legal basis to request access to employees' devices. Disclosure rules seek to ensure that all relevant documents are placed before a court for it to reach fair decisions and are therefore crucial. However, requests to access personal devices and materials can intrude into workers' privacy. The problem can be illustrated by the case *Phones 4U Limited v EE Limited*,[16] which arose in the context of allegations of breach of competition law. Against the background of this dispute, employees and former employees were required, under Civil Procedure Rules section 31, involving disclosure and inspection of documents, to hand their personal devices and emails to the employer for inspection by the employer's IT consultants. The aim was to access work-related messages and emails in these personal devices, which could be relevant to the dispute. The involvement of IT consultants was a measure that was meant to protect privacy interests. The employees and former employees were not parties to the legal dispute but treated by the court as custodians of relevant personal materials.

They resisted the request on three grounds: they argued that the judge who ordered the disclosure did not have jurisdiction to do so, they claimed that the judge should have included in his order the fact that they had a right to refuse

12. Letter from The Rt Hon Michael Gove MP to The Rt Hon Dominic Grieve QC MP (11 September 2019) https://perma.cc/TG8E-699K.
13. R (on the application of Miller) v The Prime Minister; Cherry and others v Advocate General for Scotland [2019] UKSC 41.
14. Information Commissioner's Office, *supra* note 10.
15. See *Mr D Case v Tai Tarian*: 1601297/2018; *Wells and Solari v PNC Global Logistics* [2019] EWHC 2996 (QB); *Forse & Ors v Secarma Ltd* [2019] EWCA Civ 215; *FKJ v RVT & Ors* [2023] EWHC 3 (KB), (discussed further below).
16. *Phones 4U Ltd v EE Ltd & Ors* [2021] EWCA Civ 116.

the request, and they posited that the mechanism that involved IT consultants was inappropriate and disproportionate. However, the Court of Appeal rejected these grounds. On the issue of privacy particularly, the Court said: "Whilst we accept that the vast majority of the documents on the devices in question will be potentially highly personal, *it was the Custodians that will themselves have chosen to use them for business purposes in the first place*" (emphasis added).[17] The Court recognised that the request interfered with the right to private life, including highly intimate aspects of personal life, and accepted that asking independent solicitors to conduct a search would have provided stronger protection.[18] However, it accepted that having IT consultants perform the search was a proportionate measure and that, in any case, the custodians had a right to refuse the request to hand over their devices. As discussed above, the "choice" of an employee in these contexts is often hardly a choice at all.

IV. MODALITIES OF SEARCH

The above regimes all (with the potential quirky UK constitutional exception of the "humble address") have explicit limitations on the information supplied, particularly where it constitutes personal data of a third party, or may affect an individual's right to private life. However, such limitations focus on the output of the right: the information to be disclosed. Such a test often requires the candidate information to be substantively appraised, and to do so, it needs to be obtained and analysed. These regimes discussed, however, illustrate that human rights concerns that might arise in the process of the search itself may be neglected. The search itself can be an invasive activity, and can take different forms. Below, we outline some of the forms such a search typically takes when it relates to individuals' data and devices.

A. *EX ANTE* SEPARATION

The first modality of search is not really a modality at all: it is to assume the information is separated and thus easy to transmit or search through without significant privacy concerns. Some regulated sectors, such as finance, have legal regimes requiring such separation. For example, in EU market regulation (MiFID II), certain investment firms must "take all reasonable steps to prevent an employee or contractor from making, sending or receiving relevant telephone conversations

17. *ibid*, para 36.
18. *Ibid*, para 44.

and electronic communications on privately-owned equipment which the investment firm is unable to record or copy."[19] Regulatory guidance on UK FOI law and on data protection law both urge demarcation between professional and non-professional information (Information Commissioner's Office, n.d.).

Guidance has also been created and disputed in the wake of ephemeral or "disappearing" messaging services. After the COVID pandemic, UK government guidance counsels that ephemeral messaging services should rarely be used on BYOD devices for government business except for trivial or logistical matters, and even on government-managed devices, should only be used for certain classifications of business (HM Government, 2023). In the United States (US), discussion has centred on whether and under what circumstances in particular ephemeral messaging would violate the Federal Records Act and the Presidential Records Act, with some scholars arguing for the strengthening of the latter in particular in response to the widespread use of these tools (Pope, 2021). However, courts in the US have found that the Presidential Records Act creates no duty on the president to issue *ex ante* guidelines on the use of ephemeral messaging, even though the use of these tools may fall foul of the laws.[20] Such sagas highlight the grey zones that appear when attempting to regulate communications tools in practice.

Ex ante separation, while useful, is unlikely to be a watertight or realistic strategy. Smaller organisations cannot effectively manage such complex technical separations in the face of constantly changing technologies, particularly without oversight of individuals' devices. Workers themselves may have different capacities or levels of digital literacy to be able to navigate and separate content, and may be under significant pressure, which does not allow them to spend much time managing this boundary. Personal and private information does blend with professional information systems as much as the other way around, particularly for some sectors or job types. Individuals working for many organisations in scope of different search regimes may not, in practice, put down tools for one and start work for another. Their responsibilities and duties can blur, and they can be organising elements of one job while working in, and using the tools, of another.

---

19. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU OJ L 173/349, article 16(7). Interestingly, in the UK, the Financial Conduct Authority increased the scope of this Directive during transposition beyond just investment firms. See Corfield (2018); in reference to Financial Conduct Authority, *FCA Handbook: Senior management arrangements, Systems and Controls* (12 April 2023), rule SYSC 10A.1.7.
20. *Citizens for Resp & Ethics in Wash (CREW) v Trump*, 302 F Supp 3d 127, 135 (DDC 2018), *affd,* 924 F 3d 602 (DC Cir 2019) (United States).

This complexity has been recognised by regulators. Information Commissioner's Office (2022) found that the Department of Health and Social Care was "not clear about circumstances under which [staff] could use private communication channels." In that case, the Department did not regulate BYOD devices, nor did they restrict staff from using personal accounts on corporate devices (Information Commissioner's Office, 2023). In practice, not only have individuals continued to use private accounts, but they have done it in situations where their employers should have been reasonably aware that they were doing so, thus clearly bringing such information in scope of searches under, for example, FOI law.[21]

Effectively, we are in a position where *ex ante* separation is clearly encouraged by regulators as an attempt to reduce future tensions. However, this is a poor strategy for robustly avoiding such tensions in the first place.

B. INDIVIDUAL SEARCH

Regulatory guidance often counsels that individuals should be instructed to search for information within the scope of a search themselves, on their own devices (Information Commissioner's Office, 2023, n.d.). If individuals instructed to do this conceal or erase records with the intention of preventing disclosure, they can be liable to prosecution under both FOI and data protection laws, or may be held in contempt of court in the case of disclosure under civil procedure.[22]

This initially seems like a plausible route out of the maze of issues raised so far. However, in practice, many obstacles arise. The scope of information types such as personal data, or information subject to FOI, is notoriously unclear, and will be difficult for individuals to navigate, particularly those with little legal or digital literacy and lacking regulatory training. Search functionality on many apps and devices is poor, which has led to an entire industry of expensive, centralised "e-discovery" tools to attempt to compensate for these deficits.[23] This is particularly the case for encrypted messenger services, which often make it difficult to retrieve or save data from them systematically in order to protect the efficacy of functionality such as the aforementioned ephemeral messaging (MacDermott et al., 2022). This is one reason that complex access requests through communication records can cost tens or hundreds of thousands of pounds to execute.

21. Information Commissioner's Office, *supra* note 10, para 52.
22. Freedom of Information Act 2000 (United Kingdom) s 77; Data Protection Act 2018 (United Kingdom) s 173.
23. For example, Microsoft Purview eDiscovery.

Furthermore, while many of the situations covered by the above regimes are where employer and employee interests are aligned — both are subject to a third-party obligation they are unlikely to be intrinsically keen to address — there can be more adversarial situations. In such situations, particularly where the content of the messages may have consequences for the worker or for another person, incentives may point in different directions, and the employer may be taking a high risk of non-compliance by delegating the search to an employee with ulterior motives to conceal the information requested.

C. SUPERVISED SEARCH

Regulatory guidance sometimes alludes to a supervised search, where one or more people responsible for compliance — potentially a third party — are present with a worker to guide them through the process. This again is promising, but brings hurdles. The first hurdle, naturally, is cost, both in terms of worker time and of the compliance team. The second is logistics: workers not co-located with a compliance team can struggle technically to provide access to a personal device. To do so may require the employee to install further software that has privacy implications, such as screen-recording software. Such software is furthermore restricted in some messaging apps precisely to stop screenshots of content, such as apps like *Confide* that use the *ScreenShieldKit* library which restricts both screenshots and screen recording, or *Signal for Android* that provides screenshot protection (ScreenShieldKit, n.d.; Signal, n.d.). Furthermore, while in-person it might be viable for the individual whose data is being searched to browse an app for data and then physically and selectively show it to an individual only when nothing sensitive is visible, this kind of discretion can be difficult when the search occurs remotely using a screensharing tool. However, some of these aspects can be worked around by using a camera and a video call, for example, presuming the worker has a second device that they can use which, by definition, is far from guaranteed in a BYOD context. Skill of search and completeness can remain a problem where the worker takes the lead.

However, despite these flaws, this modality has significant potential for balancing interests naturalistically.

D. DEVICE OR DATA SEIZURE

Perhaps the most extreme modality of search is the seizing of relevant data or device. Sometimes this "seizure" may be silent — as in the case of iCloud above, or in the case of mobile device management techniques, whereby employers may already have access to files through a centralised enterprise system. At other

times, data will need to be extracted from the device, potentially through taking an image of the drives on the device, or a copy of the backup for analysis.

In the UK, device extraction has been most controversial in relation to its use by law enforcement. While labour law and the investigation of suspects does not compare well due to the interests at stake, it compares quite analogously to the main issue that arose during these debates: the searching of the data and devices of victims of crime, particularly victims of sexual offences. Mobile phone extraction technologies such as "cyber kiosks" have been used by law enforcement for this purpose (Privacy International, 2018). This has been highly controversial, because the legal basis used by law enforcement for this data processing has been that of consent. However, consent is difficult to establish validly in a position where vulnerable individuals are asking a police force to investigate an offence against them, and not at all valid in relation to the many individuals to whom data on a personal device may relate (The Law Society Commission on the Use of Algorithms in the Justice System, 2019). The Information Commissioner's Office (2020) wrote a particularly damning report on the practice, recommending deep reform of this process, which led to a change in statute and a statutory code of practice (Home Office, 2022).[24]

This saga highlights some of the severe and significant problems with device extraction. Data on devices relate to many people, not just the individual to whom the device belongs, and so authorisation often cannot be given to provide that data (Home Office, 2022, para 43). Data on the device may be privileged or subject to duties of confidentiality, particularly in employment fields such as law and journalism (Home Office, 2022, para 100). Individuals may simply be unaware of the sheer volume and invasiveness of data on their devices, particularly in the context of the (often illegal) mass data collection fuelling the online advertising industry, to which app and operating system creators are often party. This is typified by the role of cookies and similar technologies in the global surveillance regime, including by national security (Armitage et al., 2023). If the data is breached, the consequences for the individual can be dire, such as the significant risk of identity fraud or compromised credentials. The process of extracting data from phones in its entirety — needed to access some types of messaging devices and other data — can utilise security vulnerabilities that can leave devices exposed or out of warranty later on (Privacy International, 2019). These tools, developed for criminal law contexts where collateral damage may be acceptable, are not well suited to the employment context.

24. Police, Crime, Sentencing and Courts Act 2022, s 37.

Cloud data extraction is typically non-damaging to devices, as once technical access is possible (which it may already be to an employer), a copy can be made silently. However, this is likely to contain data that workers do not expect. Apps often "auto-backup" contents to cloud services silently and in close integration with the operating system, which can include messages and photos. Even when apps are deleted from a device, this does not necessarily propagate a deletion into the cloud, meaning that something that is visibly unavailable to a user may nonetheless be available to an employer. This in turn prevents users from effectively appraising what data they might be granting access to without having highly technical skills to probe the "back end" of applications and, in effect, peruse the same file systems that apps themselves use for storage. Such file systems are rarely designed for easy human interpretation (because that is the point of the app itself), but are parse-able by the type of enterprise software tools that employers use to search this data.

V. PRIVATE LIFE

Given how invasive the searches that we examine here can be, this section considers further their interference with the right to private life when it comes in conflict with the interests and rights of employers and third parties. Data protection law, which is engaged in the UK and EU when such a search is carried out, does not provide clear guidance on how to balance the conflicting interests. When the right to access devices is engaged, the explicit safeguards are only at a high level of generality: a balance needs to be struck between ensuring that this right does not "adversely affect the rights and freedoms of others" (such as the individual whose device is being searched)[25] and yet does not lead to "a refusal to provide all information to the data subject."[26] This three-way tension — the obligations of the employer, the rights of the searched individual, and the rights of the third-party requestor — is practically difficult to resolve, and there appears to be little further concrete guidance on how to balance these interests within the law.

25. GDPR, *supra* note 3, article 15(4).
26. GDPR, *supra* note 3, recital 63. See also Case C-579/21 *Pannki S* ECLI:EU:C:2023:501 [80]. Where other laws create search obligations, the legal basis allowing this interference with the right to data protection should, in principle, itself define the scope of the limitation on the exercise of the right concerned — see Case C-311/18, *Schrems II* ECLI:EU:C:2020:559 [175]. They do not typically do so, however, we leave the consequences of this clash for future work.

However, we can find some principles in the case law of the European Court of Human Rights (ECtHR), which should be a significant influence on national courts in assessing how to address the conflicting interests.[27] On the basis of this case law, we propose that in the instances addressed in this article, the right to private life ought to be understood as a *right to supported separation* of work and private contexts, as well as a *right to control the process of a search of data and devices*. Such control has a number of elements as well as a number of challenges.

The ECHR is a promising basis. First, the right to private life in the ECHR is set in abstract terms, and the ECHR is a "living instrument."[28] This facilitates interpretation in ways that can capture challenges set by changes in technologies and practices. Second, the ECtHR has explored the right to private life specifically in the employment context in a line of cases and interpreted it in a manner that is far broader than the right to informational privacy that we find in data protection law alone, as we explain below. For instance, in the context of the workplace, the right to private life has been described as a right to autonomy and dignity (Collins, 2021), and has even been found to protect a right to work.[29] For this reason, it can constitute the basis for redefining the boundaries of workers' private life when the employer interferes with it in such ways as we explore here.

Article 8 of the ECHR provides that everyone has the right to private life. This is not an absolute right, but a qualified one, able to be restricted subject to a test of proportionality. From early on in its case law, the Court ruled that the right to private life is not limited in a person's home but that it can also cover the workplace. In *Niemietz v Germany*,[30] the Court recognised that the line between work and private life is blurred but said that there is

> […] no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that […] it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not.[31]

27. All EU Member States, as well as the UK, are signatories to the ECHR, which currently has 46 Parties.
28. See the discussion in Letsas (2013).
29. S*idabras and Dziautas v Lithuania*, App Nos 55480/00 & 59330/00 [2004] ECHR 395. On the right to privacy at work, see generally Hendrickx & Van Bever (2013); Otto (2016, p. 82).
30. *Niemietz v Germany*, App No 13710/88, Judgment of 16 December 1992.
31. *ibid*., para 29.

Niemietz was decided some decades ago, before the technological developments upon which we focus, and before much of the extreme blurring of personal and professional boundaries that we highlight in this article. This has not eased analysis, but has heightened the importance of this principle. Building further its conception of private life in an expansive way, the Grand Chamber explained more recently that the right to private life

> […] covers the physical and psychological integrity of a person. It can therefore embrace multiple aspects of the person's physical and social identity. Article 8 protects in addition a right to personal development, and the right to establish and develop relationships with other human beings and the outside world.[32]

Additional evidence of the breadth of the right to private life in the ECHR can be found in the case law on activities that take place in public space (Mantouvalou & Collins, 2009).[33] Such activities may be covered by the right to private life. This further disconnects privacy from a spatial conception that only views as private what the worker physically conceals from the employer and the broader public. For our purposes, this opens up opportunities to consider how to address situations when there is no spatial separation, such as when workers have not attempted to keep their private device away from work, their WhatsApp messages away from their work computer, their home cloud storage isolated from their work device or their work cloud storage isolated from their home device. When the circumstances are such that the two are blurred, which is often the case nowadays, and worker have not taken active steps to conceal personal documents and other materials, the right to private life is still applicable. This would obviously cover activities taking place at home and outside working time. But what else could it cover?

A. WHAT SHOULD WORKERS REASONABLY EXPECT?

When considering the applicability of the right to private life, the main criterion that the ECtHR employs is that of a "reasonable expectation of privacy."[34] Even though this could be a good starting point because it does not focus on a spatial conception of privacy,[35] it needs to be scrutinised carefully. In the employment

32. *Denisov v Ukraine*, App No 76639/11, Grand Chamber judgment of 25 September 2018.
33. *Von Hannover v Germany*, (2005) 40 EHRR 1; *Pay v UK*, App No 32792/05, Admissibility Decision of 16 September 2008.
34. *Bărbulescu v Romania*, App No 61496/08, Grand Chamber judgment of 5 September 2017. On this, see Atkinson (2018).
35. For discussion and analysis of the spatial approach to private life in the employment context, see Mantouvalou (2008).

context, the problem is that the idea of the reasonable expectation of privacy may be taken to mean that to the extent that there is a clear privacy policy set in an employee handbook, however intrusive this policy may be, it can limit the workers' private life for there will no longer exist an expectation of privacy. In the instances that we examine here, it may mean that given that there is legislation that forms a legitimate basis for interfering with the right, and in the case where potential modalities of search are laid out (e.g., in an employee handbook), there is no reasonable expectation on the part of employees that their devices are private. Workers simply need to be informed in advance.

Being informed that one is or that one may be monitored or that one's data or device will be searched is, of course, crucial. However, in a relationship that is characterised by inequality of power, such as the employment relationship, the fact that workers may know and may even have explicitly consented to employer interference should be far from determinative.[36] It is well known that there is a relation of submission and subordination at work (Collins, 2018; Davidov, 2016), and that workers have limited power to question workplace rules set by employers. This is more acute when it comes to precarious workers, such as workers on zero-hour contracts, whose bargaining power is even more limited for they have fewer legal rights. Unless the legitimate expectation of privacy criterion is viewed as an objective standard (not one that is set according to the employer's whim), it is of limited use in the employment context. What are the implications of this for practices that we examine here, which blur the divide between work and private life?

A landmark judgment on this matter, *Bărbulescu v Romania*,[37] developed a clear test to be applied in cases involving privacy at work. *Bărbulescu* examined the applicant's dismissal for using his work Yahoo Messenger for private communications. He had set up the account at his employer's request and even though he had agreed not to use it for private purposes, the employer found out that he had used it for private, even intimate communications with his wife and brother, and dismissed him.

In *Bărbulescu*, the Court outlined a list of requirements with which the employer should comply when there is an intrusion in workers' privacy. The requirements are clear advance notification of and/or consideration as to: (i) the nature of the monitoring; (ii) the extent of the monitoring and the degree of intrusion; (iii) whether the employer has provided legitimate reasons to justify

36. For thoughtful analysis of the value of consent in the employment context, see Niezna & Davidov (2023).

37. *Bărbulescu*, *supra* note 34.

monitoring and accessing the information; (iv) examination of possibility of using less intrusive methods; (v) the consequences of the monitoring for the employee subjected to it and the use of the results of the monitoring; (vi) whether the employee has adequate safeguards; and (vii) access to a remedy before a judicial body that can determine how these criteria are observed and whether the measures are lawful.

Having established these conditions, then, the Grand Chamber of the Court added that workers' "private social life" at work "cannot be reduced to zero."[38] This makes it clear that there is a normative threshold for privacy at work, an objectively defined core, which cannot be wiped out by notification by the employer and other related criteria. The considerations that determine the extent of workers' private social life at work which cannot be reduced to zero need to be investigated further.

The topic at hand is a potent space to explore these considerations. While the topic of this article might seem rare and arcane for the average employee (compared to, say, general employee monitoring), it is a moment where the employer has the possibility, if not precluded by appropriate safeguards, to rummage through not just aspects of the worker's private life occurring within the workplace, but aspects of the worker's life that are distinct from the workplace but, due to technological practices, have become informationally entwined with work activities. Unlike dismissal for social media activity, the nature of much of the information in this search could *never* seriously be considered "public." Unlike searching through what a worker might have said, this situation is more analogous to an employer searching through a person's home.

What more precise safeguards may be needed when the employer accesses a worker's device or cloud storage? The closest case at the ECtHR to this is *Libert v France*,[39] a case that also involves a work device that contained personal material. The applicant, who was in charge of general surveillance at the national railway company SNCF, found out that during a period that he had been suspended from work, his work computer had been seized and searched. A large number of pornographic images and films — over 700MB — were found on the hard disk. The search occurred despite that he had stored these materials in a folder named "fun" ("*rires*") within the D:/ drive, and that the label for this entire drive he had renamed "personal data." As a result of this finding, he was dismissed.

The applicant claimed that the fact that the hard drive was searched *without him being present* violated his right to private life under the ECHR. The first

38. *Bărbulescu*, *supra* note 34, para. 80.
39. *Libert v France,* App No 588/13, Judgment of 2 July 2018.

question for the Strasbourg Court was whether the search was in accordance with the law. The ECtHR observed that the French *Cour de Cassation* had ruled in a separate case that for a search of files that are labelled as "personal" to take place, the employee had to be present unless there is a serious risk or other exceptional circumstances.[40] This followed a string of domestic cases in France which started from a high level of worker privacy, and has been diluted over time (albeit still to a clearer place than many jurisdictions). In *Nikon*, a presumption of privacy within professional computer messaging was established on the basis that an employee cannot legally be prevented from having private communications on a work device, even if the employer wishes to mandate such a prohibition.[41] However, French courts moved away from such a protective presumption over time — to the delight of employers — settling eventually in *Monsieur X v Y & R* on a position that only files explicitly marked as personal by the employee should benefit from a position of prohibition of search by default.[42] Such a position is reflected in the guidance of the French data protection authority, the CNIL. They indicate that while employers have a duty to search through data to identify personal data, if a data protection subject access request is made by a worker, there is a special situation where they come across a file that individual had marked as "personal," whereby they should return the email to the requestor without inspecting it (Commission Nationale de l'Informatique et des Libertés, 2022).

Even though Libert had separated out his files, marking both the drive as personal (although using the language of the *Cour de Cassation* of "personal data" rather than of his employer who said that it should be marked "private"), the ECtHR accepted that SNCF could mount a search in accordance with the law because marking the whole drive as personal left them little other choice, and that the choice of words ("personal" versus "private") differed from their own policies.

On the question of whether the employer had a legitimate aim in *Libert*, the Court accepted that this was the case given that the employer has a right to ensure that work equipment is used in line with its contracts and other regulations. When it came to the test of proportionality for the restriction of Libert's right, the Court referred to its margin of appreciation, considered the rulings of the national courts which had taken into account the right considerations (such as the fact that the nature of his job would have required him to be a role model in

40. *ibid.*, para 44.
41. *Cour de cassation*, chambre sociale, du 2 octobre 2001, 99-42.942.
42. *Cour de cassation*, civile, chambre sociale, 19 juin 2013, 12-12.138, ECLI:FR:CCASS:2013:SO01103.

that respect and the fact that the pornographic materials took a lot of space on the D:\ drive), and found that there had been no violation of the right to private life.

The fact that *Libert* involved pornographic materials made the case more difficult than had it been about other private materials, such as personal, private, and intimate photos, and probably affected the Court's decision to recognise a margin of appreciation to the French authorities.[43] A better approach to searches of private materials on a work device is to be found in *FKJ v RVT*[44] of the High Court of England and Wales. This involved alleged hacking of WhatsApp messages by a solicitor's former law firm in the context of a legal dispute between her and a partner of the law firm. In the employment tribunal, about 18,000 WhatsApp messages were used as evidence against her. She brought a case to the High Court alleging that her former employer hacked her WhatsApp messages, and that this constituted misuse of private information. The Court explained that "[i]t cannot be seriously contested that the claimant had a reasonable expectation of privacy in her WhatsApp messages,"[45] while it also emphasised that even if she voluntarily downloaded these messages on her work computer, they would not lose their character as private materials. It explained that the material obtained enabled the defendants to "rove through several years of the claimant's day-to-day communications on all aspects of her life with those closest to her,"[46] as the claimant's lawyers put it, and highlighted that out of the 18,000 messages that they obtained, only 40 were used before the employment tribunal.[47]

The case law of the ECtHR, to conclude this subsection, contains a number of principles that are sensitive to the particularities of the employment relationship and provide a good basis to further develop our inquiry. These principles include the idea that the employee is an autonomous person who has a right to private life at work, including when using the employer's resources, that the employer can only limit the right to private life if there is a legitimate aim, subject to a strict test of proportionality and with a number of safeguards in place, and finally, that in any case privacy at work cannot be reduced to zero, particularly when some of the most intimate aspects of private life are involved.

---

43. It is common for courts to do this in cases that may raise sex-related issues. See also *Pay v UK*, App No 32792/05, Judgment of 16 September 2008.
44. *FKJ v RVT & Ors* [2023] EWHC 3 (KB).
45. *ibid.*, para 11.
46. *ibid.*, para 13.
47. *ibid.*, para 11.

B. SEARCHING FOR SAFEGUARDS FOR SEARCHES

Against this background and drawing on the above worker-protective principles on worker privacy, given that often in the cases that we discuss in this article the employer may have a legitimate ground to seek access to private devices, messages, or storage, it is important to develop a right of the worker to privacy understood as a right to supported separation and a right to control the process of a search. We first consider practices that can give this power *ex ante* — before the obligation to search is invoked — in order to limit the frequency of the problem. We then turn to safeguards that need to exist *ex post*, namely after the legal obligation to search arises, for example, during a search of someone's private device or storage where there is no clear separation of work and private materials.

1. THE RIGHT TO PRIVATE LIFE AS A RIGHT TO SUPPORTED SEPARATION

For all workplaces, employers should inform workers about the importance of such separation, and should support their digital literacy, providing training that explains the dangers of the blurring and ways in which workers can protect their private materials and communications. To some degree, this interplays with emerging legal regimes around the *right to disconnect*, which are designed to give workers greater freedom to reflect upon and strengthen the divides between personal and private life.[48]

Yet, as discussed above, such separation may often not happen because it is impracticable, time-consuming, and for other such reasons. Individuals increasingly practice complex personal forms of digital separation of different aspects of their lives, particularly to avoid "context collapse," where these areas fall into each other, but they are not always successful in doing so (Boyd, 2002; Marwick & Boyd, 2011). The tools that workers use may simply not be easily equipped to facilitate some of the separation that could support them in maintaining their privacy during a search. Consider the marking of files as "personal" in accordance with the case law of the French *Cour de Cassation*. As part of their jobs, many workers no longer interact with file systems, which have become increasingly mediated through applications that abstract away the management of information, and make it unclear what is being saved as a record and when. Younger generations reportedly struggle to understand the old metaphors of files on computers, as platforms like iOS hide their file systems from users' view (Chin, 2021). For users of mobile devices, in one study, 20% had never renamed a file on their phone, and the process is often quite hidden, for

48. See, *e.g.*, Fair Work Act 2009 s 333M (Australia); on European regimes, see generally Lerouge & Trujillo Pons (2022). See also Collins (2025).

example, files within WhatsApp (Adavi & Acker, 2023). While "sensitivity labels" exist and can be applied on emails in Microsoft Outlook (about which workers may not know), no such similar labels exist for messages on Microsoft Teams, WhatsApp, or similar individual messages, and it is not clear how workers would exclude such messages from a search. Legal regimes that require explicit renaming and relabelling seem to be at odds with contemporary technological practices.

This situation may call for more than simply providing education to employees. Law could and should play a role in facilitating a world where separation of work and life is practically easier. A few methods might promote this. At the supply-side, a design obligation could be placed on certain operators of designated tools that are common in the workplace to oblige them to make separation both easy and possible. This broadly falls in line with literature in human–computer interaction, which calls for designers to better facilitate the separation and management of different contexts, whether it be work or personal, different friendship groups, or friends and family (Nouwens et al., 2017; Van Kleek et al., 2015). Such supply-side law is increasingly common in technology law. For example, the EU AI Act places obligations designed to support fundamental rights on providers of monitoring systems to employers, but does not place many obligations on employers themselves. The logic is that such law can help motivated employers, intrinsically or by other laws, to uphold human rights.[49] Standardisation processes may be useful in this regard, insofar as they might identify state-of-the-art methods for this (which could, for example, include automatic classification or prompting of users based on language modelling of their messages that happens privately, on their devices). A co-regulatory approach would be a softer method (Marsden, 2011), which would see industry actors encouraged to create an adequate standard in the shadow of a legal regime that could apply were they not to do so sufficiently. In contrast, a demand-side obligation might see employers required to only purchase tools that adequately allow individuals to split the professional and the personal. However, not only is purchasing power often limited in the face of large technology behemoths, but this would also not tackle the issues caused by shadow IT infrastructures such as those described in Section II, as employers by definition do *not* procure these, and therefore have little power over them. A combination of both supply and demand methods is possible too, and may be appropriate given that the best

49. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) OJ L, title III and annex III, para 4.

manner of dividing the personal and the professional may be context-sensitive and may need to be worked out *in situ* rather than in the abstract.

2. THE RIGHT TO PRIVATE LIFE AS A RIGHT TO CONTROL THE PROCESS OF A SEARCH

Ex post, then, and during the process of a search of private devices, a central condition that needs to be met is that workers should not only be generally informed, or even concretely informed about a search that will take place, but that they either undertake the search themselves, or they should be present so that they give access only to materials that are strictly relevant to the search. The fact that often we are talking about people's private devices or communications, which may contain a vast amount of highly personal and sensitive documents and materials, makes it essential for workers to be present and in control of the situation. In a case such as *Libert*, had the device that was searched been private, the search and resulting dismissal would have been a clear violation of his right to private life. Moreover, in contrast to what the Court of Appeal ruled in *Phones 4U Ltd v EE Ltd*, which we discussed earlier,[50] when a court examines potentially illegal conduct, it should not be agents of the employer undertaking a search of personal devices (in that case, the firm's IT consultants), but independent third parties who can guarantee fairness in the process of a search and minimal intrusion with highly personal and irrelevant materials to the alleged illegal conduct (such as independent solicitors).

Such provisions could be enacted in a variety of ways. Courts might develop them on the basis of principles of workplace privacy that we identified in the case law above. In addition, the most promising way that we see, at least in the UK and EU, would be to add national safeguards in data protection law. In the UK, these can be easily achieved through primary legislation. Turning to EU Member States, Article 88 of the General Data Protection Regulation (GDPR) allows them to add additional safeguards in the context of employment through either collective agreements or through national law (Abraha, 2024). Such an approach could also deal with concerns from scholars that data protection law deals poorly with employee–employer dynamics in a number of areas (Albin, 2025).

A challenge here is that technologies are often not designed to be easily searchable, even with supervision. Current tools for "e-discovery" and similar compliance technologies do not envisage co-operative, privacy sensitive discovery with workers, but typify centralised managerialism and co-ordinated control.

50. *Mr D Case*; *Wells and Solari*; *Forse & Ors*; *FKJ*, *supra* note 15.

We could imagine similar design obligations to those we described above helping us out here — perhaps a "searchability by design" to accompany "data protection by design," "privacy by design," or "security by design" — an obligation on employers to have regard to tools that enable compliance in ways that are sensitive to the right to privacy. However, this too becomes difficult because by definition we are talking about private storage and communication channels over which the employer does not have design responsibility. Governance of private communications channels already seems like a daunting task (and one that digital labour platforms must somehow navigate in the Directive on Platform Work) (Veale et al., 2023).[51] Obligations of this kind would have to be structured in such a way that would propagate broadly and support individuals even when using technology that was not chosen by their employers.

VI. CONCLUSION

In this article, we have identified a new and serious challenge for workers' right to privacy. This is partly due to technological advancements that have made work more efficient, and partly due to a range of legal regimes that promote legitimate aims but that can also ground a legitimate request to access workers' data and devices. We have explained that workers' private life is blurred with their work life in ways that most people do not appreciate, and that employers may interfere with privacy in order to secure the rights of others. As we have seen, UK and EU law do not contain clear and sufficient safeguards to protect workers during the process of searching data and devices, leaving workers vulnerable to intrusions with some of the most intimate aspects of their private life. However, the scope of private life at work as it has been interpreted thus far in European human rights law is capacious. On its basis, we have suggested ways in which privacy should further be developed as a right to have supported separation of work and private contexts, as well as a right to control the process of a search of data and devices. Technology creates possibilities, and can empower workers. However, it also increases the power of employers. Legal regimes that mediate can create and facilitate undesirable power dynamics, but have so far been understudied in that context. It is therefore crucial that there are clear safeguards in place to protect workers from interference with their personal and even most intimate aspects of their private life, particularly where many competing legitimate rights are in play and at stake.

51. Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work [2024] OJ L.

VII. REFERENCES

Abraha, H. H. (2024). Hauptpersonalrat der Lehrerinnen: Article 88 GDPR and the interplay between EU and Member State employee data protection rules. *The Modern Law Review*, *87*(2), 484–496. https://doi.org/10.1111/1468-2230.12849

Adavi, K. A. K., & Acker, A. (2023). What is a file on a phone? Personal information management practices amongst WhatsApp users. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW2), Article 372, 1–28. https://doi.org/10.1145/3610221

Albin, E. (2025). The three-tier structural legal deficit undermining the protection of employees' personal data in the workplace. *Oxford Journal of Legal Studies*, *45*(1), 81–107. https://doi.org/10.1093/ojls/gqae033

Aloisi, A., & De Stefano, V. (2022). *Your boss is an algorithm: Artificial intelligence, platform work and labour*. Hart Publishing. https://doi.org/10.5040/9781509953219

Armitage, C., Botton, N., Dejeu-Castang, L., & Lemoine, L. (2023). *Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers: Final report*. Publications Office of the European Union. https://data.europa.eu/doi/10.2759/294673

Atkinson, J. (2018). Workplace monitoring and the right to private life at work. *Modern Law Review*, *81*(4), 688–700. https://doi.org/10.1111/1468-2230.12357

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data, and the public good: Frameworks for engagement* (pp. 44–75). Cambridge University Press. https://doi.org/10.1017/cbo9781107590205.004

Bietti, E. (2020). Consent as a free pass: Platform power and the limits of the informational turn. *Pace Law Review*, *40*(1), 310–398. https://doi.org/10.58948/2331-3528.2013

Blair, L. (2018). Contextualizing bring your own device policies. *Journal of Corporation Law*, *44*(1), 151–170. https://jcl.law.uiowa.edu/sites/jcl.law.uiowa.edu/files/2021-08/Blair_Final_Web.pdf

Bogg, A., Collins, H., Davies, A. C. L., & Mantouvalou, V. (2024). *Human rights at work: Reimagining employment law*. Hart Publishing. https://doi.org/10.5040/9781509938766

Boyd, D. (2002). *Faceted Id/entity: Managing representation in a digital world* [Doctoral dissertation, Massachusetts Institute of Technology]. https://www.media.mit.edu/publications/faceted-identity-managing-representation-in-a-digital-world/

Chin, M. (2021, September 22*). Students who grew up with search engines might change STEM education forever.* The Verge. https://www.theverge.com/22684730/students-file-folder-directory-structure-education-gen-z

Collins, H. (2018). Is the contract of employment illiberal? In H. Collins, G. Lester, & V. Mantouvalou (Eds.), *Philosophical foundations of labour law* (pp. 48–67). Oxford University Press. https://doi.org/10.1093/oso/9780198825272.003.0003

Collins, H. (2021). An emerging human right against unjustified dismissal. *Industrial Law Journal*, *50*(1), 36–69. https://doi.org/10.1093/indlaw/dwaa003

Collins, H. (2025). Privacy and the right to (dis)connect. *Comparative Labor Law & Policy Journal*, *45*(3), In this issue.

Commission Nationale de l'Informatique et des Libertés. (2022, January 5). *Le droit d'accès des salariés à leurs données et aux courriels professionnels*. CNIL. https://www.cnil.fr/fr/le-droit-dacces-des-salaries-leurs-donnees-et-aux-courriels-professionnels

Cook, C. (2011, September 19). *Gove faces probe over private e-mails.* Financial Times. https://www.ft.com/content/cc4b8272-e2c4-11e0-897a-00144feabdc0

Corfield, G. (2018, January 8). *FCA "gold-plates" EU rule, hits BYOD across entire UK finance sector.* The Register. https://www.theregister.com/2018/01/08/fca_mifid_gold_plating_bans_byod/

Dalla Corte, L. (2019). Scoping personal data: Towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1). https://ejlt.org/index.php/ejlt/article/view/672/909

Davidov, G. (2016). *A purposive approach to labour law*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198759034.001.0001

Durrant, T., Lilly, A., & Tingay, P. (2022). *WhatsApp in government: How ministers and officials should use messaging apps — and how they shouldn't*. Institute for Government. https://www.instituteforgovernment.org.uk/sites/default/files/publications/whatsapp-in-government.pdf

Dutton, W. H. (1999). *Society on the line: Information politics in the digital age*. Oxford University Press.

Ekbia, H. R., & Nardi, B. A. (2017). *Heteromation, and other stories of computing and capitalism*. MIT Press. https://doi.org/10.7551/mitpress/10767.001.0001

Ellison, N. B. (2004). *Telework and social change: How technology is reshaping the boundaries between home and work*. Praeger. https://doi.org/10.5040/9798216024132

Eustace, A. (2025). Bring your whole self into work, keep your whole self out. *European Labour Law Journal*, *16*(1), 74–86. https://doi.org/10.1177/20319525241312773

Griggio, C. F., Nouwens, M., & Klokmose, C. N. (2022). Caught in the network: The impact of WhatsApp's 2021 privacy policy update on users' messaging app ecosystems. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*, Article 104, 1–23. https://doi.org/10.1145/3491102.3502032

Gulacti, U., Lok, U., Hatipoglu, S., & Polat, H. (2016). An analysis of WhatsApp usage for communication between consulting and emergency physicians. *Journal of Medical Systems*, *40*(6), 130. https://doi.org/10.1007/s10916-016-0483-8

Haag, S. (2015). Appearance of dark clouds? — An empirical analysis of users' shadow sourcing of cloud services. *Proceedings of the Wirtschaftsinformatik 2015 Conference*, 1438–1452. https://aisel.aisnet.org/wi2015/96

Harris, J., Ives, B., & Junglas, I. (2012). IT consumerization: When gadgets turn into enterprise IT tools. *MIS Quarterly Executive*, *11*(3), 99–112. https://aisel.aisnet.org/misqe/vol11/iss3/4/

Hendrickx, F., & Van Bever, A. (2013). Article 8 ECHR: Judicial patterns of employment privacy protection. In F. Dorssemont, K. Lörcher, & I. Schömann (Eds.), *The European Convention on Human Rights and the employment relation* (pp. 183–208). Hart Publishing. https://doi.org/10.5040/9781474200301.ch-008

HM Government. (2023, March 30). *Using non-corporate communication channels (e.g. WhatsApp, private email, SMS) for government business*. GOV.UK. https://www.gov.uk/government/publications/non-corporate-communication-channels-for-government-business/using-non-corporate-communication-channels-eg-whatsapp-private-email-sms-for-government-business-html

Home Office. (2022, May 17). *Extraction of information from electronic devices: Code of practice*. GOV.UK. https://www.gov.uk/government/consultations/extraction-of-information-from-electronic-devices-code-of-practice

Information Commissioner's Office. (2020, June). *Mobile phone data extraction by police forces in England and Wales: Investigation report (Version 1.1)*. ICO. https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

Information Commissioner's Office. (2022, July). *Behind the screens — Maintaining government transparency and data security in the age of messaging apps*. ICO. https://ico.org.uk/media/about-the-ico/documents/4020886/behind-the-screens.pdf

Information Commissioner's Office. (2023, May 19). *How do we find and retrieve the relevant information?* ICO. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/

Information Commissioner's Office. (n.d.). *Official information held in non-corporate communications channels*. ICO. https://ico.org.uk/for-organisations/foi-eir-and-access-to-information/freedom-of-information-and-environmental-information-regulations/official-information-held-in-non-corporate-communications-channels/

Jimenez, J. I., & Jahankhani, H. (2020). Bring your own device: GDPR compliant or headache? The human aspect in security and privacy. In H. Jahankhani (Ed.), *Cyber security practitioner's guide* (pp. 239–273). World Scientific. https://doi.org/10.1142/9789811204463_0007

Kahvedžić, D. (2021). Digital forensics and the DSAR effect. *ERA Forum*, *22*(1), 59–73. https://doi.org/10.1007/s12027-021-00651-z

Kopper, A., & Westner, M. (2016). Towards a taxonomy for shadow IT. *Proceedings of the 22nd Americas Conference on Information Systems (AMCIS 2016)*, 1–10. https://aisel.aisnet.org/amcis2016/EndUser/Presentations/3/

Lerouge, L., & Trujillo Pons, F. (2022). Contribution to the study on the "right to disconnect" from work: Are France and Spain examples for other countries and EU law? *European Labour Law Journal*, *13*(3), 450–465. https://doi.org/10.1177/20319525221105102

Letsas, G. (2013). The ECHR as a living instrument: Its meaning and its legitimacy. In A. Føllesdal, B. Peters, & G. Ulfstein (Eds.), *Constituting Europe: The European Court of Human*

Rights in a national, European and global context (pp. 106–141). Cambridge University Press. https://doi.org/10.1017/cbo9781139169295.005

Levy, K. (2023). *Data driven: Truckers, technology, and the new workplace surveillance*. Princeton University Press. https://doi.org/10.1353/book.109251

MacDermott, Á., Heath, H., & Akinbi, A. (2022). Disappearing messages: Privacy or piracy? *CONF-IRM 2022 Proceedings* (Paper 10). https://www.conf-irm.org/conference/wp-content/uploads/2024/11/22-Conf-IRM-Proceedings.pdf

Mantouvalou, V. (2008). Human rights and unfair dismissal: Private acts in public spaces. *Modern Law Review*, *71*(6), 912–939. https://doi.org/10.1111/j.1468-2230.2008.00722.x

Mantouvalou, V. (2019). "I lost my job over a Facebook post: Was that fair?" Discipline and dismissal for social media activity. *International Journal of Comparative Labour Law and Industrial Relations*, *35*(1), 101–125. https://doi.org/10.54648/ijcl2019005

Mantouvalou, V., & Collins, H. (2009). Private life and dismissal: Pay v UK Application No 32792/05, [2009] IRLR 139 (ECtHR). *Industrial Law Journal*, *38*(1), 133–138. https://doi.org/10.1093/indlaw/dwp004

Marsden, C. T. (2011). *Internet co-regulation: European law, regulatory governance and legitimacy in cyberspace*. Cambridge University Press. https://doi.org/10.1017/CBO9780511763410

Marwick, A. E., & Boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. https://doi.org/10.1177/1461444810365313

Messenger, J. C., & Gschwind, L. (2016). Three generations of telework: New ICTs and the (r)evolution from home office to virtual office. *New Technology, Work and Employment*, *31*(3), 195–208. https://doi.org/10.1111/ntwe.12073

Microsoft. (2023, February 21). *Set up a connector to archive WhatsApp data in Microsoft 365*. Microsoft 365 Compliance Documentation. https://learn.microsoft.com/en-us/microsoft-365/compliance/archive-whatsapp-data

Microsoft. (n.d.). *Back up your folders with OneDrive*. Microsoft Support. https://support.microsoft.com/en-us/office/back-up-your-folders-with-onedrive-d61a7930-a6fb-4b95-b28a-6552e77c3057

Niezna, M., & Davidov, G. (2023). Consent in contracts of employment. *Modern Law Review*, *86*(5), 1134–1165. https://doi.org/10.1111/1468-2230.12802

Nooney, L. (2023). *The Apple II age: How the computer became personal*. University of Chicago Press. https://doi.org/10.7208/chicago/9780226816531.001.0001

Nouwens, M., Griggio, C. F., & Mackay, W. E. (2017). "WhatsApp is for family; Messenger is for friends": Communication places in app ecosystems. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*, 727–735. https://doi.org/10.1145/3025453.3025484

NTT Communications. (2016, April 12). *Shadow IT — Cloud usage a growing challenge for CIOs*. PR Newswire. https://www.prnewswire.com/news-releases/shadow-it---cloud-usage-a-growing-challenge-for-cios-575359961.html

Opperman, C. J., & Janse van Vuuren, M. (2018). WhatsApp in a clinical setting: The good, the bad and the law. *South African Journal of Bioethics and Law*, *11*(2), 102–103. 10.7196/SAJBL.2018.v11i2.00643

Otto, M. (2016). *The right to privacy in employment: A comparative analysis*. Bloomsbury Publishing. https://doi.org/10.5040/9781509906147

Paul, P. (2022, September 25). *Do not bring your "whole self" to work*. The New York Times. https://www.nytimes.com/2022/09/25/opinion/business-economics/work-office-whole-self.html

Pope, C. M. (2021). Ephemeral messaging applications and the presidency: How to keep the president from blocking the sunshine. *North Carolina Journal of Law & Technology*, *23*(1), 166–213. https://scholarship.law.unc.edu/ncjolt/vol23/iss1/5/

Privacy International. (2018). *Digital stop and search: How the UK police can secretly download everything from your mobile phone*. https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf

Privacy International. (2019). *A technical look at phone extraction*. http://privacyinternational.org/long-read/3256/technical-look-phone-extraction

Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Robbins, M. (2018). *Bring your whole self to work: How vulnerability unlocks creativity, connection, and performance*. Hay House, Inc.

Rosengren, C., & Ottosson, M. (2016). Employee monitoring in a digital context. In J. Daniels, K. Gregory, & T. McMillan Cottom (Eds.), *Digital sociologies* (pp. 181–194). Policy Press. https://doi.org/10.2307/j.ctt1t89cfr.18

Schiffer, Z. (2021, August 30). *Apple cares about privacy, unless you work at Apple*. The Verge. https://www.theverge.com/22648265/apple-employee-privacy-icloud-id

ScreenShieldKit. (n.d.). *Protect your app from screenshots*. https://screenshieldkit.com/

Signal. (n.d.). *Screen security*. Signal Support. https://support.signal.org/hc/en-us/articles/360043469312-Screen-Security

Silic, M., & Back, A. (2014). Shadow IT — A view from behind the curtain. *Computers & Security*, *45*, 274–283. https://doi.org/10.1016/j.cose.2014.06.007

Stewart, D. R. (2019). Killer apps: Vanishing messages, encrypted communications, and challenges to freedom of information laws when public officials "go dark." *Case Western Reserve Journal of Law, Technology & the Internet*, *10*(1), 1–26. https://doi.org/10.2139/ssrn.2952542

Tan, G., & Leech, A. (2021, April 20). *Hey that's personal! Handling employee DSARs and the social media dilemma.* Lexology. https://www.lexology.com/library/detail.aspx?g=7a22dcb1-ab0f-4d00-82e8-72a2b033111b

The Law Society Commission on the Use of Algorithms in the Justice System. (2019, June 4). *Algorithms in the criminal justice system*. The Law Society of England and Wales. https://www.lawsociety.org.uk/topics/research/algorithm-use-in-the-criminal-justice-system-report

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys*, *51*(2), Article 36, 1–27. https://doi.org/10.1145/3172869

United Nations Conference on Trade and Development. (2023, November 19). *Data protection and privacy legislation worldwide*. UNCTAD. https://perma.cc/7LYM-6Z2X

Van Kleek, M., Smith, D. A., Murray-Rust, D., Guy, A., O'Hara, K., Dragan, L., & Shadbolt, N. (2015, May 18). Social personal data stores: The nuclei of decentralised social machines. In *Proceedings of the 24th International Conference on World Wide Web (WWW '15 Companion)*, 1155–1160. Association for Computing Machinery. https://doi.org/10.1145/2740908.2743975

Varanasi, R. A., Vashistha, A., & Dell, N. (2021). Tag a teacher: A qualitative analysis of WhatsApp-based teacher networks in low-income Indian schools. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Article 560, 1–16. https://doi.org/10.1145/3411764.3445221

Veale, M., Silberman, M. S., & Binns, R. (2023). Fortifying the algorithmic management provisions in the proposed Platform Work Directive. *European Labour Law Journal*, *14*(2), 308–332. https://doi.org/10.1177/20319525231167983

Wang, Y., Wei, J., & Vangury, K. (2014). Bring your own device security issues and challenges. In *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, 80–85. IEEE. https://doi.org/10.1109/CCNC.2014.6866552

Woodbury, M. (1994). Freedom of information laws affect the autonomy of American universities. *Murdoch University Electronic Journal of Law*, *1*(4). https://www5.austlii.edu.au/au/journals/MurUEJL/1994/19.html

Yamin, M. M., & Katt, B. (2019). Mobile device management (MDM) technologies, issues and challenges. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 143–147. Association for Computing Machinery. https://doi.org/10.1145/3309074.3309103