The People App: Big Brother at Royal Mail

Postal worker correspondent
25 April 2024

Royal Mail postal workers will recall during our bitter 2022-23 industrial dispute the transparently disingenuous performance of then CEO Simon Thompson in front of the House of Commons Business, Energy and Industrial Strategy (BEIS) Select Committee.

When questioned about the technology that posties carry with them, Thompson was by turns evasive, feigned ignorance, and denied that Royal Mail was tracking its employees' movements while out on delivery. It was a patently false statement, one that was greeted with derision by delivery workers on the ground throughout the UK.

The Postal Digital Assistant (PDA) that we carry is both GPS-equipped and also uses GPS to record the location by "pinging" every time a Tracked item is scanned. At Prenton Delivery Office last October, workers voted to strike in defence of colleagues suspended and sacked after their PDAs were used to target them for taking their rest break in a local pub long-approved for such breaks.

But what many postal workers remain unaware of is the potentially far greater extent to which they are subject to surveillance by their employer even when they are *not at work*.

Beginning in 2021, Royal Mail began a two-year internal marketing campaign to promote its People App to employees. It was sold as a convenient way of receiving our pay details, if we chose to download the app onto our smartphone or similar device. It is part of the firm's digital transformation (cost-cutting) strategy to eventually move all HR services onto the app.

The shift from voluntary to "mandatory" employee-adoption of the People App came in late April 2023, after the Communication Workers Union (CWU) leadership vetoed our strike mandate and unveiled their pro-company national agreement co-authored with company executives at ACAS.

Royal Mail gave notice to its operational employees (workers) that it was ceasing production of paper wage slips altogether in June. Unsurprisingly, given the total lack of opposition from the CWU, this coercive tactic saw staff uptake of the People App increase from 85 percent in April 2023 to 97 percent by January 2024. The CWU bureaucracy made no public comment, despite the provision of pay details being a statutory right in UK employment law.

For an application with ostensibly bureaucratic functions—providing pay details, HR forms and policy, annual leave, plus corporate comms over the heads of the union on occasion— the People App appears to be incredibly invasive of the private lives of Royal Mail employees.

According to the permissions in the app's listing on Google Play, the app may request access to the employee's:

Calendar (add or modify calendar events and send emails to guests without owner's knowledge; read calendar events and details)

Camera (take pictures and videos)

Contacts (read contacts; find accounts on the device; modify contacts)

Location (access precise location (GPS and network-based); access approximate location (network-based)

Microphone (record audio)

Storage (modify or delete contents of SD card; read the contents of SD card).

In addition to its highly intrusive permissions, People App contains the code signature of a couple of third-party trackers, according to Exodus, a privacy audit platform for Android applications. The purpose of such trackers, the collection and sharing of behavioural data about individuals, is "a significant and ubiquitous privacy threat in mobile apps" identified by computer science academics Kollnig et al (*Internet Policy Review*, December 2021).

The two trackers detected by Exodus are Google Firebase Analytics and Tealium. The former offers "functionality like analytics, databases, messaging and crash reporting" and is present in 107,792 applications (60 percent).

Tealium appears to have a much wider remit and thus far a far smaller uptake (fewer than 1 percent of applications use it, according to Exodus). It collects user data "from any source including websites, mobile applications, devices, kiosks, servers, files and more" in order to create "actionable profiles' of app users. Tealium will use these profiles to "score" individuals "based on their likelihood to complete any behaviour (or combinations of behaviours)" selected. As application owner, Royal Mail is empowered to influence and direct employee behaviour.

In principle then, Royal Mail has a set of capabilities for spying on its employees that would be the envy (or at least equal) of any secret police force in the world. Over 100,000 employees have downloaded an app which could track their precise location; record audio and video; and read/modify their calendar, contacts, and SD card. It will also track all online activity and build a detailed profile of the user.

Rather than oppose this, the CWU appears fully on board.

The CWU's BRT&G agreement with Royal Mail enshrined the use of PDAs for "performance management". Appendix 5 of the agreement gives managers a new tool to oppressively monitor delivery workers. The intention is also clearly there to link performance to pay in future, further dividing the workforce.

The People App gives management vastly increased powers of surveillance and control of the workforce, outside working hours, and raises questions about civil liberties. The CWU is either unaware of this, or pretending to be; either way it is a dereliction of its duty which indicates it has learnt nothing from the Horizon scandal at Post Office Counters Ltd.

Nevertheless, the union can still talk a good fight, with recent social media footage including misleading titles such as "Fighting Against Workplace Surveillance", and "Your Employer May Be Spying on You". In the first of these, CWU Deputy General Secretary (Telecoms & Financial Services) Karen Rose talks about the issue of inward-facing dash cams in BT Openreach vans. She and her colleagues were only belatedly forced to "act" on the issue by an emergency resolution at Young Workers Conference, combined with a management leak/disclosure to the Openreach workforce which caused uproar on the company Workplace (Facebook) internal social media.

The CWU's "action" was to start a campaign (a political not industrial response) against the proposal, which was quickly shelved by management recognising the scale of member opposition to being spied on in their cabs at work. Nevertheless, Rose warns that dash cams will return as an issue in the future. She also argues against surveillance from a productivity or management viewpoint rather than on a principled basis of workers' right to privacy.

The very notion of civil liberties for working class people under capitalism where an employer can have this kind of 24-hour surveillance of workers is laughable, especially when the trade unions are in league with the employers.

The Postal Workers Rank-and-File Committee (PWRFC) opposes the oppressive surveillance of the corporate state. The measures used against Julian Assange and other opponents of war are part of wider state build-up against the working class. We need a rank-and-file fightback against the CWU bureaucracy that is colluding with the company to crush democracy in the union and the workplace.

We urge postal and logistics workers to attend the next online meeting of the PWRFC on April 28 at 7pm, "Oppose Royal Mail's Assault on the USO! Defeat CWU's Collusion". Register here to attend.