Tommy Tranvik, Mona Bråten*

The Visible Employee - Technological Governance and Control of the Mobile Workforce**

Field technology is electronic systems or equipment designed to capture and communicate data on workers in the field so that employers can manage, document or inspect the behavior and job performance of the mobile workforce. In this article, we argue that the deployment of various types of field technology can be interpreted as the technological realization of popular reform programs that have been introduced in the public and the private sector over the last three decades, especially risk management and New Public Management.

Further, we argue that the use of field technology implies that internal systems for governance and control migrate from the corporate to the individual level. We propose that one important effect of this migration is that the privacy (data protection) of the mobile workforce is diminished and that the power of managers is enhanced.

Our discussions and conclusions are based on a qualitative study of the effects of various field technologies in 52 private companies and public organizations in Norway.

Key words: **field technology, labor management, surveillance, privacy, power** (JEL: O33, M54, J5, K3)

Introduction

Field technology is electronic equipment (tablets, smartphones, laptops, etc.) or digital systems that capture work-related data on field workers. The data that is captured and retained provide detailed information about the location of field workers, what they do or the time they spend on completing various work assignments. After the data has been captured, it is automatically transferred to the company's computer system and made available (in real-time) to supervisors or management.

An important reason for the increasing popularity of field technology is that it may entail significant benefits for employers, for example by simplifying or streamlining the planning, performance or documentation of work, in addition to uncovering irregularities among employees. In this article, however, we will discuss other and

* Tommy Tranvik, Researcher, The Norwegian Research Center for Computers and Law, University of Oslo, St Olavs Plass 5, N-0130 Oslo, Norway, Email: tommy.tranvik@jus.uio.no
Mona Bråten (Corresponding author), Researcher, Fafo, Institute for Labour and Social Research, Borggata 2 b, N-0608 Oslo, Norway, Email: mona.braaten@fafo.no

** Article received: September 27, 2016
Revised version accepted after double blind review: June 14, 2017

 DOI: 10.5771/0935-9915-2017-3-319

more problematic effects of field technology. Research from Norway indicates, for instance, that field technology is seen by many employees as surveillance tools in the hands of management (Tranvik, 2013; Bråten, 2010). Moreover, the surveillance effect of field technology is a hotly debated issue that has gained the attention of, among others, the Norwegian Data Protection Authority, the Norwegian Federation of Trade Unions and the Ministry of Labour.

First, we will discuss how the use of field technology may imply transfer of control from employees (field workers) to employers (management) by submitting employees to new forms of electronic governance and control. Second, we will discuss how this governance and control may challenge the employees' right to privacy at work. The discussions are based on a study of how union and health and safety representatives in 52 private companies and public organizations in Norway experienced the consequences of field technology.

Our basic argument is that the effects of field technology can be understood within the framework of general programs for organizational reform that has swept through both the private and the public sector during the past few decades. These reform programs are closely related, although they usually appear under somewhat different labels, such as risk management or New Public Management.

We believe that field technology may realize many of the principles underlying these reform programs. Put differently, field technology may facilitate more top-down governance because these technical solutions imply the individualization of surveillance and the centralization of control within companies or organizations.

In the first part of the article we make a brief account of (a) prior research on the effects of electronic governance and control in the workplace, (b) our analytical framework and (c) the empirical evidence that this article is based on. Then, we discuss the use of field technology in 52 private companies and public organizations, and how its use may affect employees' privacy at work.

Control in the Workplace

Control of employees is defined as the management's ability to monitor and check work performance and other work-related activities so that deviations from prescribed norms of behavior, such as time spent on various work assignments, can be detected, corrected or sanctioned (Ball, 2010; Lyon, 2007).

There are two factors that characterize the use of field technology – electronic work equipment and digital systems that capture data on workers "in the field" – with regard to electronic control. First, information pertaining workers "in the field" that were previously hidden (totally or partially) from the management's view is now being recorded, transferred to and evaluated at a central location. Second, surveillance and control is individualized. In this way, surveillance and control is (or can be)

personal: field workers can be observed on computer screens and held accountable for the performance of their job assignments.

Previous Research

To our knowledge, there have not been conducted many empirical studies on the use of field technology in the workplace. The few studies that have been done indicate that the deployment of field technology is growing rapidly (see Bråten & Tranvik, 2012; Tranvik, 2013).

It has nevertheless been done some research on other forms of surveillance in the workplace, indicating that electronic control of employees may have adverse effects on the right to data protection and may also cause increased levels of stress, discomfort or alienation (see, for instance, Allen, Coopman, Hart, & Walker, 2007; Allmer, 2012; D'Urso, 2006; Hansson & Palm, 2005; Rosengren & Ottosson, 2016; Sewell, Barker, & Nyberg, 2012). More generally, the use of field technology may be relevant in light of the current literature on the Internet of things, and how this new infrastructure for data capture and exchange may impact privacy and data protection in the workplace (see, for instance, Weber, 2015).

Corporate Governance and Control

Unlike the research referred to above, our theoretical point of departure is that the deployment of field technology can be understood as the technical implementation of programs for organizational reform that have been introduced in the private and the public sector during the past 25-30 years. In the private sector, these reform programs are described and analyzed under headlines such as "the audit explosion" or risk management (Power, 1997, 2004). The corresponding reforms in the public sector are usually referred to as New Public Management (NPM) (see, for instance, Hood & Dixon, 2015; Hood, Rothstein, & Baldwin, 2010; Power, 2007).

Crucially, it is claimed that these reform programs introduce a culture of control within private companies or public organizations (Hood, 2011; Power, 2004). This culture is said to be characterized by new conceptions of the meaning of control. This means that the inner workings of private companies and public organizations – and their relations with external stakeholders, such as partners, customers or clients – are, to an increasing extent, structured by hierarchical systems of internal control set up, at least in part, to manage risks, i.e. factors (internal or external) that may adversely affect, particularly, earnings, performance or reputation. In these systems, the capture and processing of critical business information is vital: detailed information on business operations is the life-blood of risk-based internal controls (Hood et al., 2010). The hope is that more surveillance of business operations will improve corporate governance, strengthen the ability to make rational decisions and lead to "continuous improvements" in performance, quality of service, reputation or compliance with legal obligations (Power, 2007).

Individualized Governance and Control

The literature has paid little attention to the effects that this culture of control may have on individual employees. Some have argued that this is due to the fact that internal control systems are structured in terms of corporate governance rather than individual control (Power, 1994, 1997). However, in a field like computer security, internal control systems (for detecting, analyzing and responding to security events) are seen as potential tools for individual control because of the detailed collection of behavioral data that these systems entail (Cormack, 2016). In the same vein, we will argue that the deployment of field technology may contribute to a similar "trickle-down effect" in other areas of corporate governance: organization-wide systems for self-monitoring and management review may migrate from the corporate to the individual level. We believe that this can happen because field technology converts general principles of governance and control into technical solutions – these principles are embedded in the technology itself. Field Technology can thus be understood as the technological individualization of some of the most popular corporate governance programs in our time.

Similar arguments may also be found in theories of "the flexible labor market" (Sennett, 1999, 2003) and in parts of organization and technology literature (see, for instance, Bloom, Garicano, Sadun, & Van Reenen, 2014; Zuboff, 1988).

Research Methods and Data

The discussions in this article are based on the study of the deployment and use of field technology in 52 private companies and public organizations in Norway. In addition, 15 of the largest providers of field technology in Norway participated in the study.

The selected companies and organizations were distributed across seven industries/sectors: electrical installation/energy, cleaning, municipal home care, security, public transport (bus), trucking and road maintenance.

The collection of data was conducted as follows:

- 90 in-depth interviews with providers of field technology, union and health and safety representatives[1], mainly in the period from October 2011 to December 2012, focusing on the product functionality or the motivations behind, the reactions to and the (alleged) effects of field technology on privacy and the work environment.
- Internal documents: This material was provided by the companies and organizations that took part in this study, for instance, reports and plans regarding the

1 The roles of the health and safety and the union representatives are different. In practice, they often cooperate closely, and they seem to have a common approach to issues concerning field technology. We have therefore chosen not to distinguish between the two in our analyses, and use the term employee representatives.

deployment of field technology or e-mail communications between managers and union representatives concerning alleged misuse of data.

- Demonstration of field technology products by the providers.[2]

The Use of Field Technology

All of the 52 private companies and public organizations that participated in the study used two or more types of field technology. The use of field technology was distributed between the various industries/sectors as follows:

- Electrical installation and energy: Electronic travel logs (satellite-based systems for automatic registration of the use of company vehicles), fleet management systems and handheld computing devices (smartphones, PDA or laptop PCs) integrated with internal computer systems.
- Cleaning: Handheld digital devices (smartphones or PDA) integrated with internal computer systems, radio frequency identification (RFID) and electronic travel logs.
- Municipal home care: Handheld digital devices (smartphones or PDA) integrated with internal computer systems (such as electronic patient records).
- Security: Handheld digital devices (smartphones or PDA) integrated with internal computer systems, barcode systems (registration of work performance) and electronic travel logs.
- Public transport (bus): Fleet management systems, electronic ticketing systems with satellite-based tracking and real-time information systems (satellite-based systems that provide public information via electronic boards at bus stops – estimated arrival time – and that are also used for prioritizing bus services at junctions[3] and the recording of time of arrival to and departure from bus stops).
- Trucking: Fleet management systems, digital tachographs (satellite-based systems for automatic registration of driving time, breaks and rest periods), handheld digital devices integrated with internal computer systems and barcode systems (registration of goods during the loading and unloading of vehicles).
- Road maintenance: Integrated production management systems (satellite-based systems for the collection of production data) and handheld digital devices (smartphones or PDA) integrated with internal computer systems.

2 For a more comprehensive account of data and research methods, see Tranvik (2013) and Bråten and Tranvik (2012).

3 Real-time location data were communicated wirelessly from the satellite units in the buses to receivers integrated in the traffic lights. As the traffic lights received data on approaching buses, the lights would change, for example, from red to green.

Areas of Application

In this part of the article we will explain how field technology was used in the industries/sectors that participated in the study. Then, we will discuss how field technology can be understood as the technological implementation of core principles underpinning popular programs for organizational reform.

The discussion is structured according to field technology's three main areas of application:

1. Labor management, i.e. the centralization of decisions concerning the administration of jobs and field workers.
2. Documentation, i.e. the ability to demonstrate that the work is performed according to agreed-upon contractual terms or in compliance with legal obligations.
3. Inspection, i.e. the subsequent evaluation of information concerning the performance of field jobs and the behavior of field workers.

Labor Management

In electrical installation/energy and trucking companies, it was reported that the use of field technology was primarily (but not only) motivated by the desire to rationalize and streamline the administration of jobs and field workers. The point, as far as the employers were concerned, was that field technology provided managers or supervisors with updated information regarding the location of field workers and the status of jobs. This would facilitate the centralization of decision-making, particularly in relation to dispatching (the allocation of new assignments or the reallocation of routine assignments). Hence, or so the argument went, the deployment of field technology would strengthen competitiveness, increase earnings, secure jobs and improve the quality of service, for instance, by reducing response time.

In addition, it was reported that the safety of field workers – knowing the location of the personnel in the field in case of emergencies – was an important argument for the deployment of field technology. Less importantly, the employers promoted field technology as technical solutions that would simplify the documentation of completed assignments and the subsequent inspections of the quality of work (see discussions below).

This means that in electrical installation/energy and trucking companies the purpose of the deployment of field technology can be understood mainly in terms of labor management: the ambition was to make it easier for the companies to "move people", i.e. direct field workers and prioritize the use of field resources, in real-time. Hence, these companies primarily used field technology to achieve greater centralization of labor management.

In electrical engineering/energy companies, the use of fleet management systems entailed attempts to remotely control the scheduling and execution of field work. Rather than trusting field workers to do the scheduling and execution themselves and according to their own discretion, schedules could now be changed on instructions from managers or dispatchers observing the status and progress of jobs on computer screens. Managers or dispatchers would usually base these decisions on continuous streams of real-time information regarding the location of individual field workers, the jobs they performed and the status of job execution ("job started," "job completed," "available for new assignments," etc.). The systems could also provide access to information relating to field workers' professional qualifications and experience, for example, job history or safety training. This meant that when new jobs were reported to managers or dispatchers, these jobs could be assigned to the nearest field worker with spare capacity and the appropriate professional qualifications (work experience) or safety training. In addition, managers or dispatchers could get online access to individualized productivity statistics, for instance, the average time spent on completing different types of jobs (the difference between time of arrival and time of departure as registered by the fleet management system).

In principle, this meant that new jobs could be assigned to the "most productive" field workers. It was, however, reported that assigning jobs on the basis of individualized productivity statistics was not a common practice. Rather, data on work performance (especially time spent per job) was usually used for subsequent quality inspections, particularly in companies that had implemented bonus schemes.

In electrical installation companies, documentation and subsequent inspections of jobs were usually facilitated by the use of electronic travel logs and handheld digital devices. Electronic travel logs were either stand-alone products or separate modules in fleet management systems that automatically registered all driving done by company vehicles. The purpose of travel logs was to document whether or not vehicles were used for taxable after-hour driving. However, log data could also be used for subsequent inspections of work-related matters because the logs recorded data on the use of vehicles 24/7, for instance, where, when and for how long vehicles had been idle. Consequently, work performances could be estimated on an individual basis and compared with overall averages or standards set for the completion of various jobs (again, this was normally done by measuring the difference between field workers time of arrival at and departure from a customer's address). Moreover, production data that the field workers manually entered into handheld digital devices could be correlated with data from the travel logs to check for deviations, for instance, if manually registered data on time spent per job were consistent with similar data obtained from the travel logs. In energy companies, data from fleet management systems was used for similar purposes.

In trucking (freight transport), the labor management aspirations driving the deployment of fleet management systems were more pronounced than in electrical in-

stallation/energy companies. This was particularly the case with regard to the largest trucking companies that participated in the study. However, some of the smaller trucking companies had relatively modest labor management ambitions, and had therefore chosen not to invest in fleet management systems. Typically, these companies had only deployed field technology mandated by law, primarily digital tachograph, where the purpose was documenting and controlling compliance in relation to driving time, breaks and rest periods. In addition, trucking companies used temperature sensors in the cargo compartments when transporting refrigerated and frozen products (temperatures when transporting these types of products – milk, fish, meat, cheese, etc. – are regulated by law and must be documented).

The labor management ambitions expressed by the larger trucking companies were reported to be similar to those already discussed: the hope was that fleet management systems would lead to greater centralization, rationalization and streamlining of the administration of jobs, vehicles and drivers. In addition, and as in electrical installation/energy, increased personnel safety (localization of vehicles and drivers in case accidents, robbery, motor breakdown, etc.) was reported to be an important argument for the deployment of fleet management systems.

Managers or dispatchers could observe the movement of vehicles and the progress of jobs via computer screens in the trucking offices. The screens gave office personnel access to detailed real-time information on drivers, vehicles and cargo from a variety of data sources, i.e. different modules in the fleet management systems. This allowed for the mixing and matching of data so that managers or dispatchers could make operative decisions based on a nuanced picture of the situation "out on the road." For instance, real-time data on the location of vehicles and drivers could be matched with information about (a) the status of driving time, breaks and rest periods, (b) the availability of transport capacity on vehicles and (c) temperatures in the cargo compartments. Armed with this knowledge, managers or dispatchers could assign jobs according to a number of criteria, for example, the current location of drivers (new job to the nearest driver), how much driving time the drivers had left before having to take breaks or rest periods (new job to the driver with the most driving time left) or the availability of free transport capacity (new job to the driver with the most surplus capacity). Similarly, sensor data on temperature changes in the cargo department, in combination with information about the location of drivers and the vehicles' surplus capacity, could trigger instructions to reload frozen goods to the nearest vehicle with free capacity if the temperature data indicated a problem with the cooling system in one of the other vehicles.

Finally, some of the trucking companies used route optimization programs: software that planned routes and estimated (or prescribed) the total driving time and the driving time between stops along the route. If drivers deviated from the route or spent more time completing the route (or between stops) than the program had estimated, managers or dispatchers would be notified (usually in the form of pop-up

messages on their computer screens). It was reported that management had guaranteed that this information would only be used for administrative purposes, i.e. the adjustment of routes. However, it was not uncommon that the information was put to other uses, in particular to evaluate work performances: whether and why different drivers spent more or less time completing the same route.

Documentation and Inspection

In the other industries/sectors, i.e. cleaning, municipal home care, security, public transport (bus) and road maintenance, labor management ambitions were reported to be more moderate than in industries/sectors discussed above. Instead, field technology was mainly used for the purpose of documenting work and subsequent inspection of the quality of work (and, to some extent, to ensure the safety of field workers). The primary objective, therefore, was not the centralization and rationalization of administrative tasks. Rather, the objectives can be described as defensive: the capture and retention of field data in order to demonstrate that work had been done in accordance with contractual or other agreements with the customer/client – and to correct deviation if it was not the case.

In these industries/sectors (cleaning, municipal home care, security, public transport and road maintenance), the capture of field data was first and foremost based on the use of handheld digital devices (with some exceptions, see below).[4] Especially in occupations where employees left behind no visible or physical evidence indicating that the job had been done, the use of field technology for defensive purposes (documenting "the invisible") was important. Security is a case in point. Here, the primary function of field technology and the capture of data was to demonstrate that the security guard had taken the rounds and checked all the important control points (windows, doors, gates, coffee makers, etc.) as stipulated in the contract with the customer. This data was recorded by the security guard as he did his rounds by using a handheld scanner to read barcode tags that had been set up at certain intervals or close to the agreed-upon control points (or both). Data on which tags had been scanned by whom and when were then wirelessly transmitted to the security company's computer system and stored there. Each month, reports based on the scanned data were issued to the customers for inspection. The same data could also be used by the company to hold security guards to account, particularly if managers suspected that the job had not been done according to contract, for example, if the guard had failed to check all the control points.

4 However, handheld digital devices could also facilitate new forms of labor management. For instance, instead of field workers organizing the execution of job assignments themselves, assignments were now registered in centralized computer systems. They were then made available to field workers via handheld devices, but the assignments could only be opened and executed in a fixed sequence and/or on a specific date decided by managers, supervisors or dispatchers.

The safety of guards, especially those working alone or at night, was an important concern for the security companies. Therefore, handheld digital devices usually include alarm buttons or motion sensors that, when triggered, would notify colleges at the station so they could call for assistance. In addition, the devices provided for direct voice communication between security guards and the station in case of an emergency.

In cleaning services and the municipal home care, handheld digital devices was used in a similar fashion. Particularly in cleaning it was reported that RFID systems had been deployed in order to document attendance and the timing of jobs. This was accomplished by setting up small computer chips (RFID tags) at entrances and exits of buildings or rooms. Passages in and out were then automatically recorded and time-stamped on the cleaners' smartphone apps. Thus, attendance and the duration of jobs could be documented if customers alleged that the work had not been done. These electronic time records could also be used for subsequent inspections of individual work performances, for instance, by matching recorded data with contractual quality of service obligations (minutes per job). Some cleaning services even experimented with the use of digital pedometers (smartphone apps). The pedometers recorded the cleaners' physical movements (number of steps) while performing jobs, the purpose of which was to check whether or not the employees solved their cleaning tasks in an efficient manner (the optimal number of steps were estimated for each building/room and correlated with the actual number of steps recorded on the smartphone apps).

Despite the fact that handheld digital devices offered relatively extensive possibilities for the documentation and subsequent inspection of job performances, it was reported that some of the cleaning services were not particularly active in exploring these possibilities. Employee representatives suggested that the reason for this may have been that the electronic time records demonstrated "in black and white" that many employees often worked more hours than what they got paid for.

In municipal home care, field technology had primarily been deployed as a means to document that the clients (elderly, disabled, etc.) got the assistance (cleaning, cooking, personal hygiene and so on) that they had been awarded by the local authorities, measured as the number of minutes allotted to each client. Hence, measuring the duration of service was important. Even so, this was a relatively low-tech routine: assistants "ticked off" their own comings and goings on smartphones or PDAs. The recorded time difference between "ticking in" and "ticking out" indicated whether or not the various clients had received their allotted minutes of assistance.

This system and the data that it generated could be used for subsequent inspections, for instance, by measuring time spent travelling from one client to the next (the time difference between "ticking out" at client A and "ticking in" at client B). Assistants could therefore be held accountable for excessive use of time travelling be-

tween clients. However, it was reported that these types of inspections rarely happened: managers or supervisors were simply too busy to take the time to go through and evaluate each individual record. What was more relevant was using the records for identifying and assessing systematic deviations, i.e. clients with whom assistants over a longer period spent more time than the number of minutes allotted by the local authorities. Such deviations could indicate a need for scaling up or down the amount of assistance that these clients received.

Bus services in Norway are usually outsourced by local authorities to private companies bidding for contracts. The bus companies that participated in the study had all deployed fleet management systems. Contrary to the electrical installation/energy companies discussed earlier, the systems were not used for labor management purposes to any significant extent (the management of vehicles was largely determined by the timetables). Instead, the fleet management systems were primarily used for the purpose of documenting and inspecting the quality of service. The two most important indicators of the quality of service was (a) punctuality (or the lack thereof) in relation to timetables and (b) excessive idling at bus terminus (engines should generally not run idle for more than two minutes). These quality-of-service data were recorded and stored in the fleet management systems. The recorded data could, among other things, be used to impose fines or grant bonus to bus companies, depending on whether or not the agreed-upon quality of service, for instance, regarding punctuality, had been achieved.

Moreover, the fleet management systems included driver behavior analytics. This implied that so-called g-sensors (motion sensors) recorded all events during the service (braking, acceleration, bumps, tilting, etc.) that exceeded a certain threshold value. The recorded data (events) were then used to score each driver, indicating whether or not the various drivers had a particularly aggressive driving style. Drivers judged to be aggressive, i.e. drivers with the highest score (most recorded events), could be called in by supervisors for follow-up and further education, while drivers with the lowest score (fewest recorded events) could expect rewards in terms of bonuses. At the time of this study, these arrangements, i.e. the singling out of "bad" and "good" drivers for special attention or rewards, had yet to be put into practice.

Finally, in road maintenance – public services outsourced by local or state authorities to private or semi-public contractors – the emphasis was also on documentation and inspection. For these purposes, a particular breed of fleet management systems (so-called integrated production management systems) had been deployed to record data on key quality-of-service indicators (production data), especially in connection with winter maintenance. This meant automatic and real-time capture of data generated during maintenance work, for instance, the salting of icy roads (when, where, by whom and the solution and amount used) or the use of snow plows (when, where and by whom). Even if the fleet management systems were originally deployed (at least, in part) in order to centralize and rationalize labor management,

it was reported they were usually not used for this purpose. Instead, the captured production data were transferred wirelessly to the principals' computer system (either the Norwegian Public Roads Administration or local authorities). Here, the data underwent analyzes and assessments to determine whether or not the maintenance work had been performed according to contract.

As indicated, the production data could be used to evaluate the work performance of individual employees. But, as we have seen, this rarely happened. Rather, the spotlight was put on the contractors as such and how they honored their contractual obligations. Nevertheless, there were exceptions: when road accidents occurred, production data were accessed and inspected to determine if the accident may have been caused by the failure of named employees, for instance, inadequate gritting or salting.

Discussion

The discussions so far have indicated that the deployment of field technology may (and often does) lead to greater centralization of labor management or the intensification of documentation and inspection of work. The impact of these changes may, however, vary somewhat across the studied industries/sectors.

Despite variations across industries/sectors, the impact of field technology seems to be that the idea of control as something positive and necessary has taken hold among employers, even in industries/sectors where the control potential of field technology is not fully utilized. Moreover, the capture of field data means that individual employees can be regarded and managed as risk factors by identifying who the valuable and who not so valuable assets are and distributing rewards and sanctions accordingly.

Further, we have seen that field technology may help solve one of the most significant challenges that the outsourcing of public service provision implies: It may make it possible to maintain greater degree of public control as the actual service provision is entrusted to private contractors. But this can lead to increasing pressures on those who actually provide these services since greater control may also mean more surveillance and less privacy.

Privacy and Field Work

One important consequence of field technology is more surveillance: managers, dispatchers or supervisors get access to data on field workers and job assignments that have previously eluded them. Crucially, field technology systems are usually not designed to ensure mutual information- and knowledge-sharing among the various parties involved. Information control, therefore, is unevenly distributed: managers, dispatchers or supervisors know certain things about field workers, but the workers may lack knowledge of what managers, dispatchers or supervisors know about

them. Consequently, the basic premise underpinning modern ideas about privacy and data protection, i.e. that people (employees) should be able to exercise influence over the collection and processing of personal information pertaining themselves (Bygrave, 2014), may be challenged by the use of field technology.

In the next sections, we will see that the deployment of field technology can weaken field workers influence over the processing of personal information.

Criticism and Resistance

The majority of employee representatives reported that the deployment and use of field technology had been met with criticism and sometimes resistance from the employees. However, the level of criticism and resistance was unevenly distributed across the industries/sectors represented in the study. It was particularly strong in electrical installation/energy companies and trucking, that is, in industries/sectors where labor management ambitions were high. Criticism and resistance seemed generally to be somewhat less common in the other industries/sectors, i.e. where documentation and inspection were the main motivations behind the use of field technology.

The questions that emerged as the most controversial, concerned the necessity of investing in field technology in the first place, and, if deemed necessary, the types of data that should be collected, what the data should be used for, the retention period and who was going to have access to the data. Employee representatives were particularly critical of how managers would use the data and how the workers would be able to control that the data was not used for purposes other than those initially intended. The argument was that when the data had been collected, it would be easy for managers to use it for such purposes, especially to sanction behavior that managers perceived as undesirable, for instance, deviations from performance targets.

The majority of respondents therefore believed that field workers would not be able to exercise much control over the managers' use of personal information. Instead, the control over the processing of field data would be rather lopsided and would strengthen the power of managers. Managers could utilize the data as it suited them, it was argued, since no effective technical or organizational barriers restricting the processing of data had been implemented. It was also reported that field workers often did not learn about how field data was used unless they were made aware of it by colleagues or when asked to account for job performances or behavior by the managers themselves.

The Use and Misuse of Data

Allegations concerning diminished control over personal information on the part of field workers were usually associated with what employee representatives described

as misuse of field data. Misuse referred to field data being used by managers to make "negative decisions" regarding individual employees, for instance, the issuing of formal warnings and (in some cases) the dismissal of workers or the termination of labor contracts. Alternatively, the misuse of field data could refer to the processing of personal information for purposes other than those for which it had been collected.

In the companies and organizations that participated in this study, the reported number of cases concerning alleged misuse of field data (or suspected misuse) was relatively high, especially in light of the fact that many of the companies and organizations had only applied field technology for a short period when this study was conducted.

Reports of alleged misuse were particularly common in industries/sectors where fleet management systems or travel logs had been deployed. Hence, in electrical installation and energy companies these reports focused on the fact that data from travel logs, originally intended to document after-hours and taxable driving with company cars, was used for other and unrelated purposes. The data could, for example, be used to check job attendance or punctuality (time of arrival at work in the morning), response time (time of arrival at customer's location) or time spent on various jobs compared with fixed performance or productivity targets. Finally, it was reported of cases where it was suspected that managers used data from fleet management systems or travel logs in preparation of personnel matters, but did not want to reveal the data source in fear of reactions from the local union.

In other cases, it was claimed that self-reported working hours (registered by field workers on handheld digital devices) were compared with data recorded in travel logs to check the accuracy of the self-reported data. If anomalies were detected, usually that the field worker reported longer hours than the log data indicated, formal warnings were given. Similarly, incidents were cited where field workers had been asked to account for the fact that log data showed that they had visited certain addresses after work or that they had not spent the night at the home address.

In trucking, resistance to the deployment of fleet management systems was reported to be significant. This was partly due to the fact that the majority of fleet management systems collected many various types of data on drivers and driving behavior and partly because managers usually had few restrictions on the use of data. However, it seemed that inadequate information and data processing routines led to suspicion of misuse being more widespread than actual misuse. Furthermore, resistance seemed not to be particularly well organized, but usually existed in the form of frustration and sometimes anger among the drivers. The employee representatives reported that they knew about episodes of misuse of data, but it was uncommon for drivers to report grievances directly to them.

Also in trucking, the most common type of alleged misuse had to do with field data being used for purposes other than those for which it had originally been collected. More specifically, fleet management data was not only used for labor management or documentation, but also to discipline drivers, for instance, by controlling the choice of driving routes and the number of stops along the routes, or to check and correct submitted timesheets. In several of the trucking companies, it was reported that newly hired drivers were not informed about the fleet management systems. Hence, they probably did not know that managers had (or could get) access to real-time location or performance data sorted by driver. Nor was it unusual for drivers to be asked critical questions by managers about the choice of routes or if the calculated driving time between stops had been exceeded.

In a number of trucking companies, it was claimed that some of the biggest and most important customers had blacklisted selected drivers: certain drivers were no longer wanted by the customers. The reason for this alleged practice was that the biggest customers could log into the companies' fleet management systems (via the Internet) and therefore had direct access to data on individual drivers. If the data indicated that some drivers performed worse than others, i.e. spent longer time completing routes or delivering goods than desired, then these drivers could be declared "persona non-grata."

In public transport, i.e. bus companies, fewer cases of misuse or suspected misuse of data were reported than in electrical installation/energy and trucking. However, there were reports of bus drivers being dialed up by traffic supervisors (over internal communication systems) and told to turn off engines (after stopping at a bus terminus) or to reduce speed. Also, resistance to the deployment of certain fleet management features, most notably driving behavior analytics, seemed to be significant. As we have seen, the idea of driving behavior analytics is to score drivers and then to call in the lowest scorers, so-called aggressive drivers, for extra training. Most employee representatives perceived this as a form of punishment rather than as useful training, but others disagreed. These voices did, however, believed that driving behavior analytics threatened drivers' privacy and diminished their control over personal information. Still, they argued that behavior analytics were "necessary evils" to improve the quality of service and to be able to win tenders for new routes.

In cleaning services, there were reports of relatively widespread skepticism regarding the deployment and use of field technology. Even so, it was not reported that privacy issues and the misuse of field data were at the forefront of attention. Instead, employee representatives were primarily concerned about field technology leading to increased workloads and more physical strain due to the implementation of tougher performance targets. These effects were not exclusively linked to the use of field technology, but had also to be seen in light of an industry characterized by "rogue players", fierce competition and tight profit margins. However, it was argued that field technology could make matters worse by facilitating tighter control with the

achievement of performance targets. On the other hand, some argued that many cleaning services were wary of field technology because the collected data could easily be used by workers to document that they worked more hours than what they got paid for. Thus, the collection of field data might force employers to pay more in wages.

Road maintenance differed from the trends discussed above. Diminished privacy due to field technology was reported to be a minor concern, particularly since employee representatives knew about very few cases of alleged misuse of production data (snow plowing, salting, gritting, etc.). Instead, it was argued that the main effect of the collection of production data was that employees were given a chance to "whitewash" themselves if managers or principals (the Norwegian Public Roads Administration or municipal authorities) put forward allegations of sloppy or improper work. Besides, it was argued that the collection of production data would be helpful in "cleaning up" a somewhat rogue industry, i.e. smaller maintenance companies won tenders because they intentionally reported production data that gave an erroneously rosy picture of efficiency (by over-reporting how much snow removal, salting, gritting, etc. that they had done within a given time period). The hope, therefore, was that the new field technology systems and tighter control with production would lead to fairer competitive bidding in the industry.

Similarly, in municipal home care it was reported of few episodes regarding misuse of field data. Nevertheless, employee representatives believed that the use of handheld digital devices could potentially lead to tighter control of work (time spent with clients or travel time between clients). However, no widespread concerns regarding diminished privacy or the misuse of field data were reported. As we have seen, this was usually explained by the fact that managers lacked the capacity to check individual work records, or that this was only done on concrete suspicion of serious breaches of duties.

In security companies, the attitudes towards the effects of field technology on worker privacy were more critical. Employee representatives referred to several incidents of what they regarded as unjustified use of field data to make negative decisions about individual employees. In these cases, security guards had been given formal warnings by management because it was claimed that they had not completed their inspection rounds as outlined in contracts with the customers.

Summary

The discussions above indicate that a majority of employee representatives saw field technology as actually or potentially undermining the privacy of employees, in particular by reducing field workers' influence over the collection and further processing of personal information. This was also true, at least to some extent, in companies or industries/sectors where there were few reported incidents of management misuse of field data. However, in industries/sectors where field technology was pri-

marily used for documentation and inspection, it seemed that the privacy problem was viewed as somewhat less urgent than in industries/sectors where labor management was the main motivation for investing in field technology.

Conclusions

In this article, we have argued that the deployment and use of field technology can be understood as the technological implementation of principles underlying popular organizational reform programs, especially risk management and New Public Management. We have tried to show that the main effect of field technology is that workers are increasingly regarded as risk factors: data is collected for purposes of labor management, documentation or inspection so that behavior and performance can be controlled and managed in ways that are believed to minimize "waste and slack" and maximize the achievement of objectives. Also, we found no systematic variations between private companies and public institutions. Nevertheless, the outsourcing of public service seems to go hand-in-hand with tougher demands on private companies to produce detailed accounts of how individual employees carry out publicly funded tasks.

In companies that have explored the governance-and-control possibilities offered by field technology, we found that the privacy of employees is often put under pressure because of increased surveillance. Increased surveillance implies that control over personal information, i.e. field data, is transferred from the employees themselves to the companies employing them. Diminished privacy for field workers seemed to be a more salient issue in industries or sectors where individualized labor management was the main motivation behind the implementation of field technology compared with industries or sectors where this was not the case.

What we have not discussed are the likely long-term effects of field technology, particularly how it may impact the strength of unions. First, and as we have argued, the deployment of field technology may strengthen the employer's ability to organize, direct and control the work process. The position of unions may therefore be weakened: unions can, to some extent, be sidestepped as issues that were previously handled at the bargaining table may, in the future, be unilaterally decided by employers. Second, field technology may contribute to greater conflicts of interest among the union membership since individual employees can be singled out for preferential treatment or sanctions (Lysgaard, 1961).

These developments indicate that the politicization of field technology that we have seen during the last few years, at least in Norway, may be a harbinger of what will happen as more powerful instruments for data capture and exchange are likely to be introduced in the workplace. New policy or legal frameworks, for instance, EUs general data protection regulation seems unlikely to adequately address these challenges. It may therefore be up to the parties themselves – employers and employees – to navigate this increasingly complicated terrain as best they can.

References

Allen, M. W., Coopman, S.J., Hart, J. L., & Walker, K.L. (2007). Workplace surveillance and-managing privacy boundaries. *Management Communication Quarterly*, *21*(2), 172–200.

Allmer, T. (2012). *Towards a critical theory of surveillance in international capitalism*. Frankfurt am Main: Peter Lang.

Ball, K. (2010). Workplace surveillance: An overview. *Labour History*, *51*(1), 87–106.

Bloom, N., Garicano, L., Sadun, R., & Van Reenen, J. (2014). The distinct effects of information and communication technology on firm organization. *Management Science*, *60*(12), 2859-2885.

Bråten, M. (2010). *Kontroll og overvåking i arbeidslivet* [Control and monitoring in working life]. Oslo: Fafo.

Bråten, M., & Tranvik, T. (2012). *Kontroll med ansatte utenfor fast arbeidssted* [Control with employees working outside permanent workplaces]. Oslo: Fafo.

Bygrave, L. A. (2014). *Data privacy law. An international perspective*. Oxford: Oxford University Press.

Cormack, A. (2016). Incident response. Protecting individual rights under the general data protection regulation. *Script*, *13*(3), 258-282.

D'Urso, S. C. (2006). Who's watching us at work. Toward a structural-perceptual model of electronic monitoring and surveillance in organizations. *Communication Theory*, *16*(3), 281-303.

Hansson, S. O., & Palm, E. (Eds.) (2005). *The ethics of workplace privacy*. Brussels: P.I.E. Peter Lang

Hood, C. (2011). *The blame game: Spin, bureaucracy and self-preservation in government.* Princeton: Princeton University Press.

Hood, C., Rothstein, H., & Baldwin, R. (2010). *The government of risk: Understanding risk regulation regimes*. Oxford: Oxford University Press.

Hood, C. & Dixon, R. (2015). *A government that worked better and cost less?* Oxford: Oxford University Press.

Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge: Polity Press.

Lysgaard, S. (1961). *Arbeiderkollektivet. En studie i de underordnedes sosiologi* [The workers collective. A study in the sociology of the subordinates]. Oslo: Universitetsforlaget.

Power, M. (1994). *The audit explosion*. London: Demos.

Power, M. (1997). *The audit society: Rituals of verification*. Oxford: Oxford University Press.

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. London: Demos.

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press.

Rosengren, C., & Ottosson, M. (2016). Employee monitoring in a digital context. In J. Daniels, K. Gregory & T. M. Cottom (Eds.), *Digital sociologies* (181-194). Bristol: Policy Press.

Sennett, R. (2003). *Respect. The formation of character in a world of inequality*. London: Allen Lane.

Sennett, R. (1999). *The corrosion of character. The personal consequences of work in the new economy*. New York: W. W. Norton.

Sewell, G., Barker, J. R., & Nyberg, D. (2012). Working under intensive surveillance. When does 'measuring everything that moves' become intolerable? *Human Relations*, *65*(2), 189–215.

Tranvik, T. (2013). *Det gjennomsiktige arbeidslivet. Erfaringer med feltteknologi i utvalgte yrker* [Transparent companies. The use of field technologies in selected professions]. Oslo: CompLex.

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law and Security Review, 31*(5), 618-627.

Zuboff, S. (1988). *In the age of the smart machine. The future of work and power*. Oxford: Heinemann.