JOURNAL OF MANAGEMENT STUDIES

Journal of Management Studies ••:•• Month 2022
doi:10.1111/joms.12893

In the Riptide of Control and Trust: Emergence of Control Practices, Suspicion, and Distrust in New Technology Deployment

Pia Hurmelinna-Laukkanen[a,b], **Elina Niemimaa**[c], **Anniina Rantakari**[a] and **Nina Helander**[c]

[a] *University of Oulu;* [b] *LUT University;* [c] *Tampere University*

ABSTRACT In this study, we focus on the unintended consequences of new technology deployment for control-trust dynamics. When addressing these dynamics, managers and management researchers often focus on consciously designed and implemented controls and management actions that build, repair, or preserve trust. At the same time, unowned processes – processes that have no single source or purpose – easily go unnoticed. These processes may have effects that are inadvertent and sometimes detrimental. A close-up ethnographic study of a technology deployment provides insight into the emergence of unintended control practices and shifts in trust. Our findings demonstrate how deployment of new technology prompted a shift in the loci and forms of control and how trust, suspicion, and distrust surfaced asymmetrically as organizational members interpreted in different ways how others were using the new technological features. These developments contributed to the emergence of four unintended control practices: incidental monitoring, organizational surveillance, individual concealment, and collective resistance. Our study highlights the role of unowned processes in the control-trust dynamics and emphasizes that whether or not control and trust are consciously addressed, both play interactive and evolving roles in organizations.

Keywords: control, emergence, practice, trust, technology deployment

Address for reprints: Pia Hurmelinna-Laukkanen, Oulu Business School, University of Oulu, PO Box 4600, 90014 Oulu, Finland (pia.hurmelinna@oulu.fi).

The second and third authors are listed alphabetically reflecting their equal contribution to this paper. The second author as the field researcher has contributed specifically to data collection and analysis, and the contribution of the third author has emphasis on conceptual and theoretical development.

INTRODUCTION

> It was on a Tuesday morning in 2017 when my colleague, an information security expert, asked me to come to his desk. I walked over to see a graph showing the number of chats, calls, messages, and meetings of each employee in the organization we were working for. A list below the graph showed the files each employee had accessed, opened intranet pages, and chat channels used at any time, both during and outside working hours. 'Why do we see this?' he asked, and added, 'We don't need this data for the sake of information security'.
>
> Shortly after this, I learned more about how the IT admin portal made it possible to create an activity timeline for any individual user from login to logout. Hearing about this, my colleague stated that 'This surveillance – or even the mere possibility to monitor [organizational members] – has a great influence on [the organization] and how work is done here'. I agreed: I had always understood that technology can be used to control a variety of activities, but the possibility of such wide-ranging surveillance of employees and their conduct was confusing, to say the least.

Control-trust research (Costa and Bijlsma-Frankema, 2007; Long, 2021; Long and Sitkin, 2018) has established that managers' intentional attempts to adjust control and trust impact the commitment, motivation, cooperation, and performance of organizational members (den Hartog et al., 2002; Long and Sitkin, 2006). Managerial efforts for control and trust are particularly important during organizational disruptions such as the introduction of new technology (Gustafsson et al., 2021; Lines et al., 2005; Nienaber et al., 2021). However, technology deployment also can have unintended consequences for control-trust dynamics. Such consequences occur at all organizations, but easily go unnoticed. At the same time, they may cause notable damage or lost opportunities if not addressed. As prior research has shown how new technology may alter organizational control practices (de Vaujany et al., 2021; Sewell and Taskin, 2015; Zuboff, 2015) and influence the development of organizational trust (Höddinghaus and Hertel, 2021; Holland et al., 2015; Nienaber et al., 2021), scholars are now challenged to consider what unintended effects technologies may introduce at the intersection of control and trust.

In this study, we focus on the unintended consequences of new technology deployment for both control and trust and especially their dynamics, thereby looking beyond managerial action for control and trust. Acknowledging that technology deployment represents a breakdown in established organizational practices (Sandberg and Tsoukas, 2011), we examine how it may initiate changes in the loci and forms of control (Sewell and Taskin, 2015; Zuboff, 2015) and prompt shifts in trust – including development of suspicion and distrust (Bijlsma-Frankema et al., 2015; Gustafsson et al., 2021; Lines et al., 2005). A close-up ethnographic study (van Hulst, 2008) reporting the experiences of an information security (from here on, InfoSec) expert working at a financial organization (FinCo; a pseudonym) provides insight into the emergence of unintended control practices and shifts in trust.

Drawing from practice-oriented control research (Brivot and Gendron, 2011; Sewell and Taskin, 2015; Zuboff, 2015), we approach *control* as a relational practice

(Cooper, 2005) whereby organizational members regulate both their own behaviour and that of others in relation to organizational objectives (Delbridge and Ezzamel, 2005). For us, practices are not merely unrelated patterns of isolated and instantial behaviours; instead, they are emergent and have circular causal effects. Following prior trust research, we refer to *trust* as a psychological state encompassing the intention to accept vulnerability based on positive expectations regarding reliable conduct on the part of another (Long and Sitkin, 2018; Rousseau et al., 1998). These expectations arise from positive perceptions of the other's ability, benevolence, and integrity (Mayer et al., 1995). In contrast, *distrust* refers to an unwillingness to accept vulnerability owing to negative perceptions and expectations of others' abilities, benevolence, and integrity, as well as their motives, intentions, or behaviours (Bijlsma-Frankema et al., 2015). Finally, we consider *suspicion* to reflect a state of suspended judgement between trust and distrust (Capitano and Cunningham, 2018).

Our study contributes to control-trust research (Costa and Bijlsma-Frankema, 2007; Long and Sitkin, 2006, 2018) by highlighting unintentionality and emergence as relevant aspects of control-trust dynamics. Shifting our gaze away from managerial attempts to adjust control and trust, we illustrate how unintended control practices emerge in *unowned processes*, that is, processes that do not have a single identifiable source or purpose and that may reflect a multiplicity of values (MacKay and Chia, 2013). Distinctive to unowned processes is that they entail choice, chance, and their unintended consequences, taking place of their own accord regardless of human intentions and containing their own internal dynamics that no single actor controls (Chia, 2014; Langley et al., 2013). Our study demonstrates that not all controls are consciously designed and that awareness of their social interpretation and effects may be quite limited – depending on the trust environment. We advance research on control-trust dynamics (Long, 2021; Long and Sitkin, 2018) by explicitly including unintended control practices and their trust implications in the discussions on control-trust dynamics, and by showing the importance of unowned processes in parallel with deliberate managerial action.

TECHNOLOGY AND CONTROL-TRUST DYNAMICS

Implications of Technological Developments for Control and Trust

Control-trust dynamics is one of the key mechanisms in organizations (Long and Sitkin, 2006). As control and trust have multiple dimensions and occur at a number of levels (Long and Sitkin, 2018; Weibel et al., 2016), their relationships are naturally intricate. Control and trust are sometimes considered complementary and sometimes substitutive; sometimes nearly inseparable, but in other instances barely connected (Long, 2021; Möllering, 2005). This complex relatedness means that different forms of control may promote or disrupt trust and distrust, or vice versa, to various extents (Gillespie and Siebert, 2017; Long and Sitkin, 2006; Weibel et al., 2016). It also means that disruptions such as technological advancements may initiate varying changes in control and trust, or their dynamics.

Introduction of new technologies may free organizational members from spatial and temporal constraints (Aroles et al., 2019; Puranam et al., 2014), altering organizational control, and allow managers to provide autonomy, signifying trust in subordinates (Brower et al., 2009; Colquitt and Rodell, 2011; Sitkin et al., 2020). Nevertheless, technological changes also increase uncertainty. Technology may lead to 'reordering of control', in which control takes new forms and is enacted by different actors to different extents than before (Sewell and Taskin, 2015, p. 1525; see also Chown, 2021; Zuboff, 2015, 2019). Practice-oriented studies have suggested that the locus of control can shift such that control is exerted horizontally, outside managerial gaze (Ball and Wilson, 2000; Sewell, 1998), with colleagues and peers acting as surveillance agents both intentionally and unintentionally (Bauman and Lyon, 2013; Brivot and Gendron, 2011). Independent of locus, studies have reported an increasing variety in the forms of control, including peer monitoring (Brivot and Gendron, 2011; Loughry and Tosi, 2008) and technological surveillance (Newlands, 2021; Zuboff, 2015).

While monitoring and surveillance carry various meanings (Lyon, 2001; Stanton, 2000), we define *monitoring* as viewing, observing, and keeping track of an activity or condition using instruments that have no effect on what is being monitored, and *surveillance* as a more pervasive activity involving continuous (also retrospective) observation to gather information and direct someone and/or something. We consider monitoring and surveillance inherently neutral (Lyon, 2001), although we acknowledge that they typically are contrasted with privacy and freedom (Aroles et al., 2019; Zuboff, 2015) and often carry negative connotations rooted in managerial pessimism about the controlees' intentions and behaviours (Sitkin et al., 2020).

How technology is used also has implications for trust (Gustafsson et al., 2021; Höddinghaus and Hertel, 2021; Thielsch et al., 2018). Technological advancements have been connected to shifts in managers' trust in employees, employees' trust in their peers, managers, and organizations (Holland et al., 2015; Long and Sitkin, 2018; Searle et al., 2011), and trust in technologies (Hengstler et al., 2016; McKnight et al., 2011). When organizational members learn to use and cope with new technology, they need to be willing to feel vulnerable and develop positive expectations that it will lead to better outcomes and not harm them or their organizations (Nienaber et al., 2021). Importantly, organizations run notable risks when they fail to acknowledge the changes in organizational culture that come with new technology deployment (see Lessig, 2006). Individuals' attempts to cope with the changes brought about by technology may prompt colliding interpretations and views between managers and employees, resulting in employees' unwillingness to cooperate, problematic behaviours such as vigilantism, or suspicion and distrust (Cui and Jiao, 2019; DeCelles and Aquino, 2020; Sørensen et al., 2011). For example, information security may be perceived in quite divergent ways (Hedström et al., 2011; Janssen et al., 2020; Rainer Jr et al., 2007).

Among the unwelcome outcomes, distrust is particularly problematic. Distrust is considered to persist in a self-amplifying cycle across an organization (Bijlsma-Frankema et al., 2015; Sørensen et al., 2011), fed especially by perceptions of value incongruence, the belief that others hold incompatible values (Guo et al., 2015; Sitkin and Bijlsma-Frankema, 2018). Trust, suspicion, and distrust may evolve unevenly – generating trust asymmetries across an organization as individuals experience varying access, exposure, and insight to changes and interpret the changes in different ways (Gillespie and Siebert, 2017). Because of the differences in individual experiences and interpretations, managers may not be able to identify the reasons for distrust (Gillespie and Siebert, 2017; Sitkin and Bijlsma-Frankema, 2018) or the point at which suspicion or low-level trust deteriorates into distrust (Bijlsma-Frankema et al., 2015), which makes distrust challenging to prevent or repair.

Addressing the Changes Brought by Technology

Acknowledging the need for managerial attention and action, existing studies provide insight into managerial efforts to influence control and trust (Long, 2018; Reed, 2001; Simons, 1994; Sitkin et al., 2020; Whitener et al., 1998), including the effects of technological changes on control and trust from the managerial point of view (Höddinghaus and Hertel, 2021; Holland et al., 2015; Nienaber et al., 2021). However, limited attention has been paid to emergence and unintentionality in control-trust dynamics. New technologies have been noted to come with unplanned consequences (Lessig, 2006) and they may hence alter control-trust dynamics in unexpected ways. For example, they entail risks such as 'surveillance creep', where technologies are used for wider surveillance than initially intended (Ball, 2010). As a result, organizational members may accept necessary aspects of technological control, but simultaneously experience suspicion and distrust due to increasing vulnerability (Nienaber et al., 2021; Sitkin and Bijlsma-Frankema, 2018) and oppose more intrusive components through avoidance, obfuscation, and resistance (Newlands, 2021).

We argue that process organization research (Chia and Holt, 2006; MacKay and Chia, 2013) provides useful starting points to understand and address emergence and unintentionality in control-trust dynamics. This research highlights the role of unowned processes that do not have a single identifiable source or purpose (MacKay and Chia, 2013) and unintended practices that are not purposeful and goal-oriented, but adaptive and emergent, as outcomes of unowned processes (Chia and Holt, 2006). Drawing on these discussions allows us to capture consistent patterns (rather than instantial behaviours) of organizational action and reaction that occur also beyond intentional and formal practices. Hence, we argue that this view offers a more comprehensive account also on how control-trust dynamics evolve. These aspects form a central part of our empirical examination.

EMPIRICAL INSIGHTS – INTRODUCTION OF NEW TECHNOLOGY

Research Design

Our study draws from close-up ethnographic material (Järventie-Thesleff et al., 2016; van Hulst, 2008) collected by one of the authors, a field researcher who worked at the research site, FinCo, as an information security (InfoSec) expert when new technology was being deployed. The materials offer insight into a role of organizational actors who lack direct supervisory authority over employees but yet have a position to exert control, thereby allowing examination of diagonal control (next to its vertical and horizontal forms). The material also contains discrete observations of various professional groups, which has been found valuable in studies on the development of distrust (Bijlsma-Frankema et al., 2015). These materials provide a rare real-time view of how change unfolded in an organization, avoiding the limitation of having retrospective material only (see Bijlsma-Frankema et al., 2015; Gustafsson et al., 2021). While ethnography does not allow establishing definite causal relations, it is considered useful in studying the fluidity of organizational processes (Emerson et al., 1995; van Hulst et al., 2017). Our empirical material captures the chronological unfolding of relevant events, revealing shifting control-trust dynamics and the emergence of unintended control practices.

Collection of Empirical Material

The analysed empirical material is part of a wider ethnographic work conducted by the field researcher on information security policy implementation. It consists of extensive field notes (comprising both direct *observation notes* of speech and occurrences, and the *field researcher's personal notes* entailing interpretation of various encounters), documentation from official meetings and workshops, and group and individual interviews (see Appendix). The field researcher spent over a year during 2016–17 working as an InfoSec expert at FinCo, returning later to the organization in 2018 and 2019.

We focused on the materials collected during an eight-month period in 2016 and 2017 when the new technology was deployed. During this period, the field researcher spent from one to three (most often two) days per week at FinCo, doing her work, listening to people, collaborating with them, and observing organizational members and their practices at meetings, workshops, and lunch and coffee breaks (see Ingold, 2014). An announcement made in the organization and reminders in interviews ensured that the employees of the organization were aware that the field researcher was also conducting research.

The time spent at the organization allowed the field researcher to gain an intimate understanding of daily activities and practices at FinCo. Her tasks as an InfoSec expert connected her to various organizational members, enabling her to observe their behaviours and learn about their perceptions and attitudes. From her expert position, the field researcher was able to closely follow the adoption of new technology and its effects. She had access to sensitive information and took part in organization-level meetings related to control, monitoring, and the breadth of surveillance. The field researcher also used and evaluated the technology from the InfoSec perspective. Observation initially focused on information security practices pertaining to adoption of the new technology. As the project continued, feelings, experiences, and actions related to control became visible, including indications of trust. These developments were recorded in the materials, providing unique real-time insight.

Research Context: Introducing New Technology in a Financial Organization

FinCo is a large financial services provider that offers wealth management solutions in Finland. FinCo has a results-oriented culture where hard work is appreciated. Although FinCo operates in a highly regulated field, management does not monitor how employees achieve their objectives and exerts control only if expectations are not met. This is part of the company's culture and typical of corporate culture in Nordic countries that score high in general trust (see Bernstrøm and Svare, 2017). Reflecting the high-trust environment, FinCo has received an external commendation for its employee friendliness.

In the financial service industry, information security is an integral issue. Despite the generally high levels of trust, in the past company personnel were expected to work at FinCo's offices to reduce the risk of data breaches. Use of the intranet and internal company IT systems was technically possible only inside the offices. Working from home or in the public sphere was also prohibited by company policy. Phone calls and limited access to email were the only communication methods outside the offices.

In 2016 FinCo's top management decided to provide employees with tools for working outside office spaces and pursued increased overall productivity by introducing a cloud-based technology platform, Microsoft Office 365 (O365), offering intranet, extranet, office tools, email and various other communication tools (see Table I) on a server accessible from outside the office.

Table I. The technological context: deployed O365 tools

Tools introduced with O365	*General purpose of the tool*	*Use at FinCo*
Email and shared spaces	Communication and collaboration	Email was used to send messages in a fashion similar to the email system used before introduction of O365. Shared spaces provided organizational members with the ability to share and work jointly on documents and other materials.
Skype/ Teams	Communication and collaboration tool (later replaced by Teams and similar solutions).	Skype and Teams were used to communicate with others and share materials. They were also used to observe other users' presence and activity.
Delve	Tool used for searching information across O365 applications.	Delve provided FinCo's employees with the ability, for example, to search for documents and people in their organization and a means for employees to see on which (parts of) documents their colleagues (and customers) were working on.
Admin portal	The O365 admin portal offers a view of the applications introduced and insight into the types of activities employees and management conduct with O365 applications. If offers a view, for example, on how many people communicate with Teams, how many meetings a particular employee organizes and participates in. It shows statistics on chat communications.	IT experts used the Admin portal to observe the use of applications and to track possible technological problems.

At the time of the technology deployment at FinCo, many organizations were moving from local to cloud servers, and security concerns were raised on many fronts (Stieninger et al., 2014). On the other hand, the overall benefits of cloud computing had been acknowledged both generally, and at FinCo. Deployment at FinCo appeared to entail a relatively straightforward change from one technological solution to another; beyond increasing temporal and spatial freedom, no notable alterations were expected in core tasks or organizational relations. Table II summarizes the key changes in the methods and contents of work that resulted from introduction of the new technology.

The technology deployment affected organizational members in different ways. FinCo has specific organizational groups that have distinct expertise, are responsible for varying organizational functions, have diverse daily practices, and played different roles in O365 deployment: Top management (responsible for strategic decision-making), experts (InfoSec and IT experts), professionals (financial and legal), and operational employees (customer service). While management made the decision to deploy the technology in line with the objective of improving performance, the IT and InfoSec experts had the goal to make sure that the change was efficient and safe, and were assigned the tasks of implementing the changes in technology and in company policy, respectively. Professionals and customer

Table II. Changes in the organizational context resulting from O365 deployment

Change domain	*Before technology deployment*	*New technology deployment*	*After technology deployment*
Places of working	Work was done at the office spaces using IT systems and tools that allowed access only from the office spaces and within normal office hours.	O365 allowed access to email, intranet, and different collaboration tools from anywhere.	Most of the professional work is independent of place. Customer service still works from the office space.
Working times	Most work was done during office hours.	O365 allowed access to email, intranet, and different collaboration tools at all times.	Some work is independent of time; Working time is determined more by customers' needs.
Transparency to others' work	Employees mostly saw the end products or results of others' work.	O365 offered various collaboration tools (Skype, Teams, shared virtual spaces, Delve) that allowed employees to work simultaneously on different documents (e.g., contracts, customer information) and provided transparency to see who is working on what (a document or a specific part of a document, for example) and when. Online presence became visible.	Employees could not only on the end products or results of work, but also others' intermediate outputs and work processes. Contents, times, and ways of working were also visible. The visibility extended also beyond the organization's boundaries (to customers).

service employees were expected, and trusted, to continue their work, now aided by O365. Table III provides an illustrative summary.

Analysis of the Empirical Material

Before the actual analysis of the empirical material, the field researcher constructed a chronological timeline (see Langley, 1999) to map out the key events in the process of deploying O365 at FinCo. The timeline describes the main events related to deployment of the new technology, highlighting the point of view of information security (Figure 1). The timeline and context descriptions provided by the field researcher provided the research team a first view to the unfolding of events. It also served as a point of reference at later stages of analyses.

In the early stages of our study, we faced a practical challenge. Some ethnographic material was confidential and could not be shared fully with the research team. The field researcher removed confidential parts from the raw records and provided the rest of the materials to the other authors.[1] To compensate for this, we had extensive iterative discussions and email communication about the observations and interpretations. We engaged in varied interaction that contributed to team sharing and allowed more thorough comprehension (Jarzabkowski et al., 2015). While the field researcher was immersed in the case, the other authors zoomed out analytically on the empirical material (Nicolini, 2009), producing new insights, asking questions, and challenging each other's interpretations (see Chang et al., 2016). This allowed extracting more details, such as information on the backgrounds and education of representatives of organizational groups.

The interaction also prompted a shared shift from the focus on information security to control and trust, and to more specific themes. While control emerged as a central issue during our first reads of the materials, with recurring references to monitoring and surveillance, when we later returned to the material to comprehend the reasons behind the emergence of control practices, a few significant individual notions directed our attention to suspicion and trust. There also were instances pointing to distrust as an implicit phenomenon. Examining how control practices emerged at FinCo became the focus of our analysis. The teamwork helped overcome the limitations of potentially self-absorbing autoethnography (Chang et al., 2016) and enabled us to gain an understanding of local practices and context while still preserving the richness of the ethnography (Jarzabkowski et al., 2015; Nicolini, 2009).

Our analysis followed an abductive, iterative approach, moving between empirical materials and theory (see Gustafsson et al., 2021; Jarzabkowski et al., 2015). To obtain an overall understanding of the nature and contents of the materials (Emerson et al., 1995; van Hulst et al., 2017), all authors read the records multiple times. When analysing the material, attention was paid to some records being objective accounts of occurrences, and others comprising subjective insights. Two authors conducted an independent thematic coding: The field researcher coded the full empirical materials, and another author did the same except for the confidential parts. The coding framework was developed in collaboration between these authors, first staying close to the material, and then ordered and aggregated to higher levels, informed by the existing literature and negotiated by the entire author team (see Gioia et al., 2013). Comparisons of code patterns did not indicate

Table III. Backgrounds of organizational members and roles in the new technology deployment

Organizational groups	*Before technology deployment*	*During technology deployment*	*After technology deployment*
Top management (*four involved in the deployment*) • Higher education in business admin and economics and finance; long-term practical experience • focus on efficiency	Directing work by monitoring and managing work output	Responsibility for making the decision to deploy the new technology; Mandated IT experts to carry out deployment in practice; Allocated assessment of information security issues to InfoSec experts	Directing work by monitoring and managing work output; Embracing and endorsing the flexibility of work allowed by the new technology
Information technology (IT) experts (ca. *ten involved in the deployment*) • Engineers with higher education and training in information and communication technologies • focus on efficacy	IT administration	Ensuring that the technological infrastructure works in a purposeful manner; Did the deployment and technical adjustment work in practice?	IT administration and monitoring of technology use; Using O365 in their tasks and in general communication and collaboration
Information security (InfoSec) experts (*CISO and four experts*) • Engineers with higher education and training in communications technology, industrial economics, and with InfoSec certifications • focus on threats to data integrity and privacy	Planning and executing InfoSec measures for preventing data breaches (e.g., with strict InfoSec policy by limiting employees' access to company information outside the office and by regulating technologies such as firewalls and antivirus software)	Preservation of the confidentiality, integrity, and availability of information; Were assigned to evaluate the new technology from the perspective of information security.	Planning and executing InfoSec measures for detecting data breaches; Using O365 in their tasks (information security solutions embedded in the organization's normal communication and working tools); Evaluation of O365 InfoSec risks considering the contexts and means of working.
Financial professionals (ca. *100*) • Higher education in finance, business admin, economics, industrial economics; experience in banking	Conducting the core functions of FinCo; Providing services to the customers of FinCo; Accessing and handling a variety of documents and materials entailing confidential and sensitive information.	Adopted O365 as one of the key tools; Started working outside of the firm premises.	Conducting the core functions of FinCo; Providing services to the customers of FinCo; Accessing and handling a variety of documents and materials entailing confidential and sensitive information.
Legal professionals (ca. *10*) • Highly specialized and experienced lawyers (university degree in law in line with formal requirements) • focus on efficiency			

Table III. (Continued)

Organizational groups	*Before technology deployment*	*During technology deployment*	*After technology deployment*
Operational level, customer service employees (ca. *40*) • Varying education, training and experience mostly in business administration	Providing customer services; The work requires their presence on the firm's premises and they had regular working hours.	Handle the routine practicalities; The systems that they used were transferred to O365 with all other groups, but the change was not particularly visible.	The work continued to require their presence on the firm's premises and they had regular working hours, also after the technology deployment

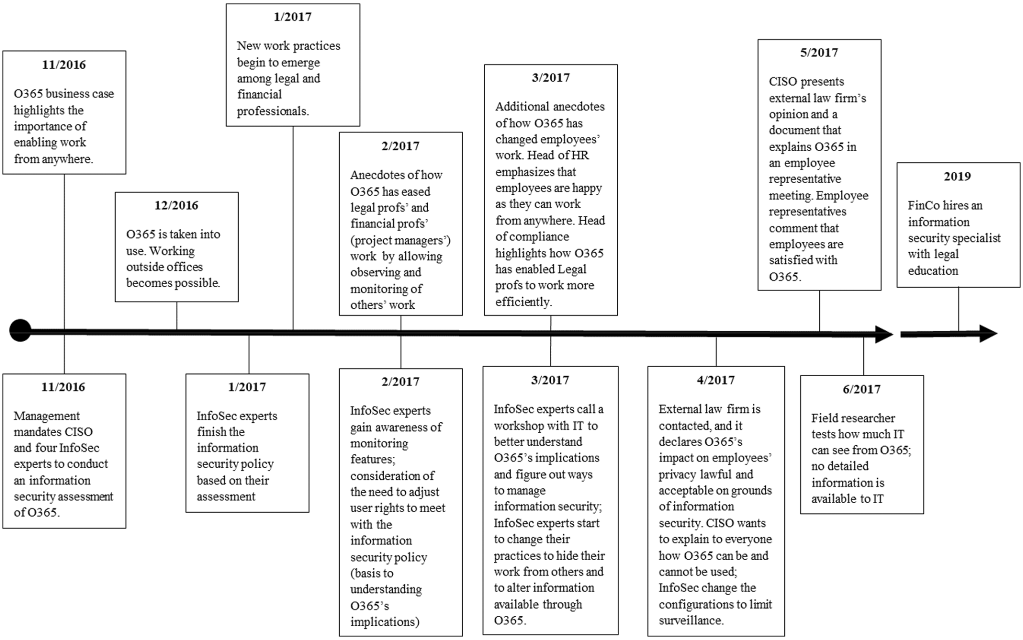
11/2016 O365 business case highlights the importance of enabling work from anywhere.
11/2016 Management mandates CISO and four InfoSec experts to conduct an information security assessment of O365.
12/2016 O365 is taken into use. Working outside offices becomes possible.
1/2017 New work practices begin to emerge among legal and financial professionals.
1/2017 InfoSec experts finish the information security policy based on their assessment
2/2017 Anecdotes of how O365 has eased legal profs' and financial profs' (project managers') work by allowing observing and monitoring of others' work
2/2017 InfoSec experts gain awareness of monitoring features; consideration of the need to adjust user rights to meet with the information security policy (basis to understanding O365's implications)
3/2017 Additional anecdotes of how O365 has changed employees' work. Head of HR emphasizes that employees are happy as they can work from anywhere. Head of compliance highlights how O365 has enabled Legal profs to work more efficiently.
3/2017 InfoSec experts call a workshop with IT to better understand O365's implications and figure out ways to manage information security; InfoSec experts start to change their practices to hide their work from others and to alter information available through O365.
4/2017 External law firm is contacted, and it declares O365's impact on employees' privacy lawful and acceptable on grounds of information security. CISO wants to explain to everyone how O365 can be and cannot be used; InfoSec change the configurations to limit surveillance.
5/2017 CISO presents external law firm's opinion and a document that explains O365 in an employee representative meeting. Employee representatives comment that employees are satisfied with O365.
6/2017 Field researcher tests how much IT can see from O365; no detailed information is available to IT
2019 FinCo hires an information security specialist with legal education

Figure 1. Timeline of the main events; Information security perspective

problems with code definitions or interpretation, although there were a few instances where the field researcher needed to provide additional information to complete the coding. For example, those parts of the material containing jargon (e.g., InfoSec-specific abbreviations) were left uncoded until the field researcher explained what they meant. Some recoding was done during reporting the findings; the first round of coding led to identifying three control practices, but later the last one was split in two (see Grodal et al., 2021). The resulting data structures (see Gioia et al., 2013) are shown in Tables IV and V.

The data structures revealed differences and similarities across the organizational groups (for example, differences in the ways the groups balanced the benefits brought by technologies with risks, and groups' varying attention to and awareness of control

Table IV. Unintended control practices

Aggregates	*2nd order codes*	*1^{st} order codes*	*Illustrative quotes (direct observation)*	*Interpretations of observations (implicit denotations)*
Incidental monitoring	Monitoring others' work habits	Professionals checking when coworkers are logged in; IT experts observing their coworkers' work habits and online presence in real time	'An IT project manager had the habit of checking from Skype which of his colleagues work during weekends' (Observation notes);	See Vignette #1; 'Skype shows who's online' (Interviews; Fin prof)
	Monitoring (changes in) contents of work	Professionals checking which documents others (peers, customers) worked on and how; looking up other people	'Earlier, I did not know if my colleagues or contract partners had done changes in the contract as agreed or when I could get it back' … '[now] Delve shows all changes' (Observation notes; Quote/ Legal prof).	See Vignette #1
Organizational surveillance	Surveillance of the functioning of the technology	IT experts continuously observing the frequency and extent of application use	'[An IT expert] introduced graphs that they produced. Those showed how many employees had been using Teams, how (chat, calls, meetings), and how often' (Observation notes).	See Vignette #2
	Surveillance of organizational members' activities	IT experts using admin portal to keep watch over individuals; checking the purpose of application use	'One IT expert demonstrated how he could reconstruct work done by an individual employee on any single day' (Observation notes).	See Vignette #2

Table IV. (Continued)

Aggregates	*2nd order codes*	*1^{st} order codes*	*Illustrative quotes (direct observation)*	*Interpretations of observations (implicit denotations)*
Individual concealment	Avoiding the use of technology	InfoSec experts not opening shared documents; reducing use of technology; stopping use of email	'[InfoSec expert] said that he logs out so that he would not be spied on' (Observation notes).	See Vignette #3; 'I decided that I would not download documents that I do not absolutely need' (Field researcher's personal notes).
	Using tactics that obscure patterns of technology use	InfoSec experts hiding their work habits; using technology irregularly to make it difficult for others to interpret what they are doing	'Skype really allows you to see who is online, but can you really draw conclusions on the working habits of others?' (Field researcher's personal notes).	See Vignette #3; '[An InfoSec expert] joked about how he will stop using Skype; he told that he will log out from Skype for the weekend, when he was planning to do some work' (Observation notes notes).
Collective resistance	Resisting unintended use of technology	InfoSec experts searching for information on appropriate monitoring and surveillance; calling attention to their privacy concerns	'CISO highlighted that it is important to inform everyone about O365 features' (Observation notes); 'This needs to be told to the [top managers]. This kind of surveillance cannot be justified' (Interviews/ InfoSec expert).	See Vignette #3; 'CISO had contacted IT managers and discussed the unauthorized deployment of Teams and the admin portal.' (Observation notes)
	Regulating technology use	InfoSec experts setting restrictions to use of technology for surveillance purposes	'We tightened [by changing the configurations] the approach with regard to IT experts so that their activities could be seen later on if misconduct from their side was suspected' (Field researcher's personal notes).	See Vignette #3 'Beyond fixing IT problems, no surveillance is allowed' (Observation notes; Quote/CISO).

Table V. Organizational trust asymmetry

Aggregates	*2nd order codes*	*1st order codes*	*Illustrative quotes (direct observation)*	*Interpretations of observations (implicit denotations)*
Culture of trust	Positive expectations	Professionals, experts, and managers trusting technology to bring benefits; ease of work acknowledged; general benevolence perceptions; Managers reducing monitoring	'I got an impression that she marks these things in Excel because she is concerned about her coworkers working too much' (Observation notes); 'It also helps improve information security' (Interviews/InfoSec expert).	See Vignette #1; 'There has been a lot of positive feedback' (Interview/HR manager); 'Freedom' (Interviews/Fin prof); 'HR director highlighted that he opposed any monitoring of employees' (Field notes).
	Accepting vulnerability	Managers expressing trust in employees; Professionals and Customer service accepting technology, monitoring, surveillance, and the need of maintaining information security; Managers sharing and delegating control	'There are risks in remote work. I fully trust our employees' (Interview/HR manager); 'I do not doubt our employees. I trust them' (Interview/manager);	'[An InfoSec expert] knows about [information security] issues' (Observation notes; Quote/Top-manager); 'IT worries about the IT risks' (Interview/top-manager); 'We need to be controlled' (Interviews/Fin prof); 'Monitoring is good [laughing]' (Interviews/Fin prof).
Suspicion	Capability concerns	InfoSec experts expressing concerns about security of the technology; concerns about other organizational members' capabilities to handle technology and to address excessive monitoring and its purposes	'[An InfoSec expert] noted that this new technology 'is not as easy to understand or handle as non-cloud technologies and therefore poses a risk' (Observation notes). 'The CISO seemed irritated (because he felt that managers did not understand what it would mean)' (Observation notes); 'Customer service does not seem to be aware of anything' (Field researcher's personal notes).	See Vignette #2; 'The fact that the applications come automatically to everyone means a loss of control over IT services' (Observation notes); 'Service providers might have access to the information [on everyone's use of technology without IT being able to stop it]' (Observation notes); '[InfoSec expert] said he could not understand where the texts and documents shared in Teams were stored and who could access them' (Observation notes).
	Integrity concerns	InfoSec experts feeling uncomfortable about Managers not paying attention to security; concerns about IT experts observing others without restrictions	'I had a feeling that IT does not use the admin portal only to fix problems, but also to surveil employees' (Field notes; Personal views); 'What could [IT experts] deduce from my workdays just by interpreting those graphs?' (Field researcher's personal notes); '[my colleague and I were laughing:] "only InfoSec experts can be this suspicious"' (Observation notes/Quote InfoSec expert); '[I considered IT experts habit of logging in to see who is online as] weird behavior' (Field researcher's personal notes).	See Vignette #3; 'When information is available like this, there is a possibility that it will be used to other purposes than intended' (Field researcher's personal notes); 'I was expecting [the possibility of surveillance] to be a big deal for the employees or managers representing them, but apparently it was not. I wonder if this is because they do not know what can be done with this technology, or if they do not care? If this is merely a positive thing for them?' (Field researcher's personal notes).

Table V. (Continued)

Aggregates	*2nd order codes*	*1st order codes*	*Illustrative quotes (direct observation)*	*Interpretations of observations (implicit denotations)*
Distrust	Not accepting vulnerability	InfoSec experts not trusting that information is safe; turning to external law firm for support; stopping activities that allow monitoring; not approving revealed actions; informing other employees	'CISO highlighted that it is important everyone understands the purposes for which O365 can be used and how it can be abused. ("Abuse" being the opinion of CISO referring to his view that the revealed conduct was not acceptable)'. (Observation notes) 'CISO asked me to contact [an external law firm] and request a statement on the use of the surveillance features' (Observation notes).	See Vignette #3; 'Today I decided to stop using the [FinCo] email on my phone; you never know if a new feature emerges that collects more information than earlier' (Field researcher's personal notes); '… we should have the possibility to monitor the provider in the O365 service agreement. We agreed that [InfoSec expert] will see to this' (Observation notes).
	Pervasiveness (within group)	InfoSec experts sharing their concerns and talking about their behaviors and perceptions; developing similar views; adoption of similar practices	'My colleague told me that he had significantly reduced the use of O365'; 'I admitted [to my colleagues] that I was also choosing very carefully what documents I downloaded' (Observation notes); 'Because Skype espionage came up again, I decided to talk to others about it' (Field researcher's personal notes).	See Vignette #3; 'InfoSec expert started to paint a picture of "the US monitoring us all"' (observation notes); 'I tested O365 today by using it and inquiring from IT experts what they had seen' (Observation notes; notes made after adding the restrictions).

influences) and helped us situate emergence of control practices and indications of trust, suspicion, and distrust on a timeline, revealing the unfolding of control-trust dynamics.[2] Providing us with further tools for understanding the control-trust dynamics, and the nature and occurrence of control practices, the field researcher wrote vignettes that described situations where the practices were particularly explicit. This recontextualization facilitated our understanding of the developments.

Findings

Our findings demonstrate how deployment of the new technology altered control-trust dynamics and resulted in the emergence of unintended control practices. The technology deployment initiated changes in the loci and forms of control (Brivot and Gendron, 2011; Sewell and Taskin, 2015) and shifts in organizational trust (Bijlsma-Frankema et al., 2015). Reflecting emergence, new control practices arose in different parts of the organization. Indications of developing trust asymmetries – the emergence of suspicion and distrust in some parts of the organization, amid a general prevalence of trust – and the related differences in attention to control influences further led us to conclude that many reactions were not intended. Below, we first describe the unintended control practices that emerged during and after introduction of the new technology. We then discuss the emergence of these practices in the light of trust asymmetries, explicating their intertwined development.

Unintended practices of control. Our ethnographic material pointed toward emergence of four unintended control practices at FinCo: *incidental monitoring, organizational surveillance, individual concealment*, and *collective resistance*. Incidental monitoring and organizational surveillance appeared to arise as direct and early results of technology development, while practices of concealment and resistance emerged only later as organizational members reacted to the unfolding of events. The following discussion and vignettes describe their main elements and features from the perspective of the field researcher working in the capacity of InfoSec expert.

Incidental monitoring. The first vignette shows how at FinCo the introduction of new technology provided organizational members with a real-time view of others' work, enabling monitoring among those using the same applications, including other employees, managers, and FinCo's customers. Incidental monitoring as a control practice at FinCo comprised (1) *monitoring the work habits of other organizational members*, and (2) *monitoring the (changes in) contents of work* (see Table IV).

Especially FinCo's legal and financial professionals took notice of work-related behaviours such as the timing and duration of online presence of those working on the same tasks. Likewise, they checked changes others made in shared documents and in this way observed what others considered important. All organizational members could see who was present online, which logically meant that they also knew they could be monitored themselves. The employees also discussed monitoring openly; 'Two IT experts noted they had seen the same person online on Saturdays. That means that they log into Skype themselves during weekends to see who is online' (Field researcher's personal notes). Although monitoring was generally infrequent, in some cases it became relatively extensive.

> Vignette #1: Mike is one of FinCo's lawyers who works on supplier and partner contracts. I was working with Mike on a contract document, when he told me that he had found Delve to be a great tool for checking whether a colleague or an employee of a partner was working on a contract draft. 'Delve tells you who has been working on a shared document', he explained, and continued: 'That's very practical as now I know when others are really working and when they are not'. Mike further told me that seeing what others were writing in the shared document gave him information about what the others saw as important. I was surprised because I only learned about Delve now.
>
> Later on, I learned more about the possibilities in O365. Tina, a financial professional, mentioned over coffee that she was worried about her team leader because he seemed to be working from 6am to 10pm. Tina had gathered this information by opening her Skype client, checking who was online and when, and recording the information on an Excel spreadsheet.
>
> These instances left me with mixed feelings. I trusted that the employees had good intentions, but I could not understand why they keep track of others' work to this extent. Somehow, I know that they are doing it for work efficiency and/or out of genuine concern for colleagues, but I still felt that it was not right.

Incidental monitoring emerged gradually as organizational members learned what O365 enabled them to do. Initially, management was unaware of this practice developing in FinCo. The monitoring seemed to be benevolent (e.g., showing concern for peers' well-being) and task-oriented: '[the legal professionals] highlighted how much this helps them understand the customers and allows them to find new ways to interact with them'. (Observation notes). Importantly, the monitoring function of O365 was used because it could be used, rather than having a specific reason; the organizational members did not set out to monitor each other but ended up doing so more and less consciously. Eventually, monitoring others seemed to become such an everyday practice that it could be brought up in coffee-table conversation.

Organizational surveillance. Organizational surveillance as a control practice differed from incidental monitoring with regard to its coverage and its continuous and covert nature. While surveillance was partially horizontal and entailed a vertical (bottom-up) aspect, it emerged mainly diagonally; the IT experts' role and de facto ability to enact control and hence influence other organizational members emerged from the sidelines, without a supervisory position or authority. At FinCo, organizational surveillance comprised *observing* (1) *the functioning of the technology* and (2) *organizational members' activities*. Notably different from the tools of incidental monitoring that were visible to organizational members, surveillance took place without those observed being aware of it. The IT experts collected and processed data from all organizational members to manage the functioning of O365, using tools visible only to themselves. Based on information compiled over time, they had an expansive view of organizational members' online activity.

Reflecting the covert nature of organizational surveillance, outside the group of IT experts, it went unnoticed until the InfoSec experts started to pay attention to how legal and financial professionals used the applications for monitoring. Motivated by the need to understand the technology's information security risks, InfoSec experts set up a meeting with IT experts to inquire about O365 features. The discussions revealed that the IT experts could carry out organization-wide surveillance and showed the extent to which some of them already used these features. The following vignette describes this.

> Vignette #2. The chief information security officer (CISO) had been informed that employees had adopted a new O365 application, Teams, that had not been authorized by management or assessed by us for information security attributes. He was puzzled about how this had happened and wondered out loud in a meeting how many employees were already using the application. Two IT experts responded: 'We can see how many people use it and how often'. They presented reports that gave detailed information about when an employee had used the tools, how many messages he or she had sent, and over which channels and how many meetings the employee had attended each day. The IT experts were excited to show us how they could reconstruct any employee's working day from the small signals gathered by the system. I was concerned about what I had seen. I realized that as O365 was becoming central for the FinCo employees' work, the IT experts could monitor everyone's behaviour from the time they logged in to O365 until the time they logged out.

Like monitoring, organizational surveillance seemed to develop unintentionally as part of work: 'IT experts had not known about the technology features allowing monitoring and surveillance in advance' (Observation notes). The InfoSec experts understood that surveillance by IT experts was meant to ensure the overall functionality of the O365 in the organization and that it mainly focused on the extent and frequency of application use (see Table IV; Surveillance of the functioning of the technology). However, the new tools also enabled surveillance of individuals and might allow sensitive information to be viewed externally ('Service providers might have access to the information'; Observation notes). For InfoSec experts focused on security and privacy these capabilities posed real risks.

Individual concealment and collective resistance. Two practices developed among InfoSec experts as they realized that the new technology features had increased uncertainty and vulnerability by enabling incidental monitoring and organizational surveillance. As a consistent reaction to the increasing risk of breaches of privacy, InfoSec experts first engaged in *individual concealment*, which comprised (1) *avoiding use of technology* and (2) *using tactics that obscured patterns of technology use*. InfoSec experts' early reaction was to move themselves away from the monitoring and surveillance. A second practice, *collective resistance*, emerged later as InfoSec experts understood what the newly emerging practices meant for the organization. Collective resistance involved (1) *resisting unintended use of technology* and (2) *regulating technology use*. In contrast to concealment – which was accomplished by self-regulation – collective resistance, characterized by explicit protesting, was intended to influence the behaviour of others. Collective resistance also emerged as a form of diagonal control, with InfoSec experts playing a central role in its emergence.

InfoSec experts realized that they did not have enough understanding about O365 to protect either the confidential information of FinCo or the privacy of the organizational members. 'We discussed the technology. "How do we manage information security for all the data and information if we don't even know what services the technology entails?"' (Observation notes; Quote/InfoSec expert); '[An InfoSec expert] had been studying the configurations and he was entirely unsure of what information is collected' (Observation notes). To cope with the vulnerability, the InfoSec experts increasingly started to avoid using applications altogether, or deliberately used the technology in ways that would conceal their actual activity (see Table IV).

Not knowing who was observing whom and when surveillance occurred seemed hardest for the InfoSec experts to accept. They were concerned about how the new technology would be used and how the information retrieved from use of the technology would be interpreted: 'I am completely stunned to see the Admin portal […] I can't help but wonder how privacy regulation correlates with this' (Field researcher's personal notes). Eventually, InfoSec experts started to collectively resist the emerging monitoring and surveillance by explicitly calling attention to their concern and by initiating concrete changes in the organization to limit the use of surveillance-enabling features of O365 (see Table IV). The final vignette describes these developments.

> Vignette #3: John, an InfoSec expert, was upset after the discussions with the IT experts: '"Shocking! I can only think of how to stop those IT guys from seeing my workday"' (Interview/InfoSec expert). I saw him engaging in an extensive search for more information about the technology's features. He also began to deliberately disconnect from Skype every now and then to ensure that 'he could not be spied on through it' (Observation notes). He also told me that he always disconnected when he worked long hours on weekends. Anders, another InfoSec expert, shared John's concern about the monitoring-enabling features. He began studying the artificial intelligence attributes of O365 because he was sure that there were features that he did not know about or could not understand. He was concerned of how data about his work on O365 was used by the service providers, worried that surveillance could in this way extend beyond FinCo. He became reluctant to use O365 at all. Having similar concerns, 'the CISO repeatedly noted that IT has a huge responsibility and highlighted that IT experts in their role as IT experts have a lot of information on the users of the technology' (Observation notes). I also found it disturbing that IT experts, or anyone with their access rights, could reconstruct my working day from the signals of my O365 usage. I had a hard time comprehending that this kind of surveillance would be justified. A problem was that management seemed to be reluctant to make any changes even if we tried to explain them the risks. In the end, we collectively decided to make configurations on O365 that would restrict what IT could do with the technology.

InfoSec experts' growing concern led them first to evade monitoring and surveillance that made them feel personally vulnerable and that they professionally considered problematic. As they shared their concerns among themselves, they became increasingly aware of the risks of internal and external surveillance and privacy breaches. Even if no malevolent behaviour or abuse of the system had been observed, InfoSec experts considered the risks of these too high.

Individual concealment and collective resistance contrasted with the management's idea of increasing flexibility. These practices also were somewhat counterintuitive considering InfoSec experts' responsibility to secure the integrity of information; these practices posed limitations not only to others' use of technology, but to InfoSec experts' own work, which benefitted from monitoring and surveillance-enabling features in detecting information security violations. However, these practices, too, inherently reflected benevolent intent; the ultimate motivation was to protect the organization and its members.

The nature of the emergence of unintended control practices. Although the new technology was deployed to add flexibility and autonomy, and although management rejected its use as a tool for managerial monitoring and surveillance, organizational control did not diminish. Instead, unintended control practices emerged through seemingly minor but consistently recurring encounters between vertically, horizontally, and diagonally connected (groups of) organizational members, and the changes in perceptions and behaviours that took place as a result. That is, unintended control practices emerged not guided by anyone specifically, or with any specific purpose. The features of O365 were used because of they could be used. Hence, the managerial choice to deploy new technology, mixed with the unexpected uses of the technology and the various reactions of different organizational members, influenced the emergence of unintended control practices. To understand these issues better, we next elaborate the differences among organizational groups regarding developments of control and trust.

Trust and control in different organizational groups

As organizational groups within FinCo had varying roles in the deployment of the technology, they experienced the change differently. Analysis of these differences revealed important aspects of control-trust dynamics during and after new technology deployment. In particular, the differences between the groups indicated how trust, suspicion, and distrust developed unevenly in the organization, generating trust asymmetry that contributed to the emergence of the unintended control practices. Table VI provides an overview of these aspects.

Management. As the new technology was introduced, top management explicitly expressed their goal to increase employee autonomy: 'Top management was determined to make the corporate culture less controlling' (Observation notes). Managers' statements reflected trust in their employees: 'There are risks in remote work. I fully trust our employees, so I do not think these risks are relevant' (Interview/HR manager). Similarly, management trusted the experts to take care of many important tasks, providing them with control over these: 'IT worries about the IT risks' (Interview/Top-manager); '[An InfoSec expert] knows about [information security] issues' (Observation notes; Quote/Top-manager).

Management repeatedly accentuated the benefits of the new technology, focusing their attention on positive feedback (see Table V; Positive expectations). Managers

Table VI. Summary. Control and trust in different organizational groups

Organizational group	*Attention to influence of technology*	*Ability to enact control through technology*	*Attention to control influences*	*Changes in trust*	*New control practices*
Management	Yes	Yes, but declined	Low. Increased when InfoSec experts raised concerns	No. Signalled trust by adding flexibility	None
Legal and financial professionals	Yes	Yes	No	No	Monitoring
Customer service	No	Yes, but not comprehended or realized	No	No	None
IT experts	Yes	Yes	No	No	Monitoring and surveillance
InfoSec experts	Yes	Yes	High	Yes. Suspicion, distrust, action to repair distrust	Concealment and resistance to curtail monitoring and surveillance

also considered the monitoring-enabling features of O365 in this light: 'It is good that employees can see each other' (Interview/HR-manager). When InfoSec experts communicated their concern about the emerging monitoring and surveillance practices, management perceived that as an unwelcome obstacle to their intention to increase flexibility: 'Changes that would reverse the positive developments were "not an option"' (Observation notes; Quote/Top manager). Managers seemed reluctant to see the potentially negative implications and risks of the new technology.

These observations demonstrate how management simultaneously signalled trust (Brower et al., 2009) and contributed to changes in the locus of control by intentionally decreasing hierarchical control and delegating certain tasks to IT and InfoSec. As a result of management's unwillingness to assume control, it trickled down to other parts of the organization (and also to stakeholders outside FinCo). Management seemed to hold fast to perceptions of the ability, benevolence, and integrity (Mayer et al., 1995) of those using the technology in their work and those responsible for its deployment. However, managers' disregard of the control implications brought by the technology unintentionally drew attention to the contradictory views between managers and InfoSec experts (Bijlsma-Frankema et al., 2015; Rainer Jr et al., 2007) and caused changes in how managers' trustworthiness was evaluated (Sitkin et al., 2020).

IT experts. Having been given the responsibility to conduct the technical deployment of O365, IT experts had the broadest perspective on how the technology worked, what information it displayed, and what actions it allowed. They valued the increase in efficiency, focusing on the aspects of surveillance that facilitated their work: 'An IT expert explained how convenient the admin portal is. According to him "it facilitates work enormously when there is no longer any guessing regarding use"' (Observation notes; Quote/IT expert).

The central, autonomous role of IT experts in technology deployment created the potential for extensive surveillance throughout the organization: 'They can surveil anyone! Me or the CEO' (Interview/InfoSec expert). However, they also seemed ignorant of the implications of these capabilities for control and privacy concerns. For example, they did not seem to realize that they might be subject to monitoring and surveillance themselves (see Table V; Capability concerns). Furthermore, IT experts seemed to be willing to trust that the new applications and updates could be deployed without closer scrutiny: 'The messages explaining [automatic updates] are terribly long "so who reads them?"' (Observation notes; Quote/IT expert). The IT experts further noted 'that new services are added on a weekly basis [and] said that they can't keep up with the new additions (expressing some frustration with the workload)' (Observation notes). By admitting this to their InfoSec colleagues, IT expects unintentionally eroded their trustworthiness regarding their integrity and ability to address potential risks related to the new technology.

The observations above imply that the focus of IT experts on tasks related to ascertaining the functioning of the technology kept them largely unaware of how their intrusive actions could be threatening to other organizational members (see Lessig, 2006; Tidd et al., 2004). In addition, management's continued expressions of trust in the IT experts insulated them from concerns about the implications of their work. However, the IT experts' apparent lack of attention to the implications of monitoring and surveillance caused concern among InfoSec experts.

Legal and financial professionals. The *legal professionals* were strikingly content: '[O365] has allowed me to find new co-workers […] I can see if they are working on [a project], and if I need to contact them' (Interviews/Legal professional). They either paid no attention to monitoring and surveillance or accepted it. When these professionals monitored others, they were not concerned about the potential that they could be monitored too: 'I really have not thought of others looking me up' (Interviews/Legal professional).

The *financial professionals* reacted similarly, considering control a natural aspect of work in the financial sector and trusting that it was appropriate (see Table V; Accepting vulnerability): 'Control just has to exist' (Interviews/Fin professional). Like the legal professionals, the financial professionals focused on improvements to their work practices: 'I can now see what kind of changes the customers need' (Observation notes; Quote/Fin professional). However, it also seems that their understanding of the control-enabling features not directly related to their work remained limited: 'Why wouldn't it be okay to check who's there; that is the purpose of Skype?' (Interviews/Fin professional). The low level of awareness and concern was noticed by the InfoSec experts: '[Financial professionals] clearly have not thought about this' (Field researcher's personal notes).

The analysed materials imply, though only indirectly, that the professionals' trust in other organizational members or in what they did with the technology did not change during the observation period. Their attention to the implications of control remained limited, and their attitudes toward the emerging control practices were positive or neutral. The professionals were interested in emerging control to the extent that it improved their daily work (see Ball, 2010; Tidd et al., 2004). While they were not explicitly expected to have the capabilities to address risks brought by the technologies, their apparent neglect of these issues can be seen to reflect different values from those of InfoSec experts.

InfoSec experts. Collected by an InfoSec expert, our ethnographic materials naturally provide the most comprehensive insight into the experiences and actions of this group. The materials demonstrate how the views of the InfoSec experts shifted during the observation period.

InfoSec experts were wary of the technology from the outset, an attitude to be expected given their goals in technology deployment. Signifying their suspicion toward the technology and its providers, InfoSec experts were concerned about maintaining information security and protecting confidential knowledge: '[An Infosec expert] worried that the features of the new technology create unwanted information leakages' (Observation notes). However, InfoSec experts also had positive expectations of the new technology's potential to facilitate their work, not only by providing flexibility ('My own work will be easier, as I can access my email easily' Field researcher's personal notes) but also by offering the means to detect security breaches and observe the ability of users to behave responsibly and carefully (see Table V; Positive expectations).

The attitudes of InfoSec experts changed gradually but significantly as they learned more about incidental monitoring practices. At first, the InfoSec experts seemed ambivalent: 'I was wondering how I should understand the monitoring features of this technology' (Field researcher's personal notes). The enthusiasm of the legal and financial professionals about the ability to monitor others puzzled the InfoSec experts: 'Why do these things raise so little emotion? Why do I feel like the [monitoring and surveillance] should be limited, but the [professionals] find them to be quite ok?' (Field researcher's personal notes). InfoSec experts explicitly acknowledged having *suspicious attitudes* (related to their inherent values and their focus on preserving information integrity) in discussions about how they had started to limit their use of O365 to adjust their visibility to others (see Table V; Integrity concerns). Still, apart from developing the practice of individual concealment (See Table IV) and trying to comprehend the newly emerged practices, the initial reactions of InfoSec experts were relatively mild; the InfoSec experts changed their own behaviours to an extent but did not pursue to influence others.

The InfoSec experts' continuing attempts to understand the technology revealed privacy risks such as the potential for surveillance creep: 'I had a feeling that IT experts do not use the admin portal only to fix problems, but also to surveil employees [to the extent of breaching their privacy]' (Field researcher's personal notes). The diverging views and behaviours between InfoSec experts and other organizational groups became more apparent over time, generating a growing within-group perception of value incongruence: 'The CISO seemed irritated by [the behaviors of top management]' (Observation notes; see also Table V; Integrity concerns). The InfoSec experts exchanged more information on their observations, feelings, and their own ways of avoiding surveillance, which manifested an increasing prevalence of negative perceptions within this group (see Table V;

Pervasiveness). Although we found no evidence of erosion of their perception that others had benevolent intentions, the notions above suggest that their trust in the integrity and capabilities of others became compromised (see Table V; Integrity concerns, Capability concerns).

Finally, the increasing negative perceptions generated explicit resistance within this group, which, in combination with their avoidance and concealment behaviours, suggests that the InfoSec experts no longer tolerated the risks or accepted vulnerability. This is consistent with *distrust developing* in this group. InfoSec experts were even willing to sacrifice the ease of their own information security work rather than let the activity continue that introduced vulnerability; even if they could have used the technology to ease their own work, they chose not to: 'The configuration improves our chances to detect information leaks if we will use all possible [features], but then IT experts would see even more of the activities of the users. […] None of [the InfoSec experts] wanted to expand monitoring and surveillance' (Observation notes). Acting on their concerns, InfoSec experts placed surveillance-limiting restrictions for organizational members (especially IT experts) (see Table IV; Regulating technology use).

The InfoSec experts also reached out to management. However, managers valued the positive developments regarding flexibility and refused to jeopardize them, which increased InfoSec experts' frustration. The field researcher retrospectively noted that this was probably because managers were worried that employees would have reacted negatively to limits placed on their achieved flexibility, possibly causing a decline in trust. Whatever the reason, these events seemed to contribute to the InfoSec experts' perception that their values were not appreciated among top-management. Moreover, InfoSec experts did not seem to trust management' capabilities to address the risks: 'When coming to the office, the CISO stated (notably troubled) that "O365 is the playground of IT" and that no-one is managing or questioning their activity in the admin portal [referring to the expectation that management should have taken action]' (Observation notes; Quote/CISO). Similarly, InfoSec experts were concerned about IT experts' capabilities based on how IT experts described their challenges with the technology and updates (see Table V; Capability concerns). Consistent with their limited trust in their FinCo colleagues' capability to adjust monitoring and surveillance to an appropriate level, InfoSec experts sought information on these issues from legal specialists outside the organization (see Table V; Not accepting vulnerability). This action also reflected the values held by InfoSec experts: '[CISO] considered it important to make sure that all activities are legal' [Observation notes].

These developments could have escalated into self-amplifying cycles of distrust across the organization. However, our case does not suggest that this happened. Instead, the findings indicate that InfoSec experts were able to rebuild a situation in which they could tolerate vulnerability and where their positive expectations exceeded the negative ones – consistent with the notions of *repairing distrust* and *restoring trust* (to a low level). Initially, the InfoSec experts did this through their own control practices to regulate technology use so that risks were mitigated. Having some agency of control, InfoSec experts could rely on individual concealment and collective resistance practices without anyone disrupting their repair attempts. The analysis suggests that even if not all concerns about monitoring and surveillance were removed, they were alleviated: 'I tested O365 today by using it and inquiring from IT experts what they had seen […] They were able to see which documents I had opened and that I had used Teams, but could not see the contents of my doings or what I had done in Delve [indicating that the goal of limiting surveillance had been achieved] (Observation notes). Later, in 2019, the management hired an information security specialist with a legal education, which concretely signified to InfoSec experts that management acknowledged security and legitimacy to be important and endorsed InfoSec's values. We interpret this as trustworthy managerial behaviour that further helped to repair the earlier distrust issues'.

Intrigued by these observations, we looked further into how and why collective resistance as a control practice did *not* seem to contribute to escalating distrust – which could be expected both intuitively and based on earlier studies (e.g., Bijlsma-Frankema et al., 2015; Nienaber et al., 2021; Sørensen et al., 2011). Our analysis indicates, first, that not only did reliance on concealment and resistance practices connect to distrust, but they also signified InfoSec experts' willingness and ability to return to a low level of trust; the inherent intention was to reduce uncertainty in the organization, not to oppose others' actions as such. This is consistent with studies showing that suspicion can originate from contextual information related to actors' behaviours, rather than the behaviours as such (Capitano and Cunningham, 2018; Fein and Hilton, 1994). Second, the role of the InfoSec experts in deployment of the technology, and especially the fact that critical evaluation (including sceptical attitudes and behaviour) was expected of them, likely obscured their developing distrust from other organizational members. In the high-trust environment, other organizational members did not seem to interpret the reactions of the InfoSec experts as signs of distrust. This context could explain why managers did not respond with negative reactions or distrust when InfoSec experts sought to verify the lawfulness of technology uses; rather, managers considered this as normal part of information security work. Likewise, instead of opposing changes, the IT experts themselves provided the information needed by the InfoSec experts to restrict surveillance: 'IT experts showed us different configurations […] which allow limiting their activities [in O365] quite widely' (Observation notes). As these behaviours signalled the benevolence of managers and IT experts, showing their willingness to help InfoSec experts to carry out their tasks, they likely reduced perceptions of value incongruence among InfoSec experts.

Customer service employees. We observed one group where deployment of O365 did not alter control-trust dynamics significantly. Customer service work revolved around customer encounters and was tied to specific working hours and location also after deployment of O365: 'In reality, the employees were using O365, but this was not really recognized' (Observation notes); 'We do not use [O365] at home' (Interviews/Customer service). Because these employees did not experience changes beyond adapting to new software, their attention to the new technology and its implications was practically non-existent: 'New? Is there some new email?' (Interviews/Customer service).

These observations are consistent with literature suggesting that ignorance and indifference are common reactions to new technology deployment and that organizational members may not pay attention to the forms of control enabled by new technologies

(Ball, 2010; Lessig, 2006; Zuboff, 2015) or the related security issues (Bulgurcu et al., 2010). Our case did not indicate that customer service employees re-evaluated their trust in management or technology. Customer service employees did not pay attention to monitoring capabilities of the new technology or changes in control, and did not experience signals indicating changes in trust, which is consistent with the observation that no control practices emerged from this group (see Table VI).

Control-trust dynamics in unowned processes. The above insights suggest how control-trust dynamics played a role in the emergence of unintended control practices in and through unowned processes entailing choice, chance, and their unintended consequences (Chia, 2014; MacKay and Chia, 2013). First, emergence of incidental monitoring and organizational surveillance practices – that originated from the technology-induced changes enabling varying actors to enact different forms of control – was inherently facilitated by the culture of trust. In the high-trust environment, limited awareness of emerging control and its implications allowed spreading of the unintended practices and restricted (immediate) opposition to them. No malevolent intent or behaviour was perceived even by InfoSec experts focused on securing confidentiality and integrity of information and tuned to detecting its misuse (Bulgurcu et al., 2010; Janssen et al., 2020). Second, where negative control interpretations did emerge, practical coping took place; individual concealment and collective resistance among InfoSec experts seemed to simultaneously result from, and manifest, suspicion and distrust (see Newlands, 2021; Sitkin and Bijlsma-Frankema, 2018). Third, control and trust also seemed to connect in halting distrust development and repairing it (Bijlsma-Frankema et al., 2015), with concealment and resistance practices used to reduce vulnerability. Aiding this, the high-trust culture in the organization preserved a perception of benevolence such that all emerging actions were assumed to be taken for better outcomes for the organization and its members. Despite the (isolated) trust erosion, the remaining elements of trustworthiness seemed to provide adequate basis for self-restoration of trust among InfoSec experts, and simultaneously to keep concealment and resistance from being retaliated by other organizational members. These insights indicate that managerial action is not necessarily needed to repair eroded trust (see Gustafsson et al., 2021) but that distrust can be mitigated when individuals have the agency and means to reduce vulnerability by enacting control. Overall, we suggest that following the logic of unowned processes (Langley et al., 2013; MacKay and Chia, 2013), control and trust play a role also without being consciously addressed, with their dynamics unfolding on their own accord regardless of human intention.

DISCUSSION

Building on and moving beyond earlier studies that have focused on the interplay between trust and vertical control exerted by managers (Costa and Bijlsma-Frankema, 2007; Long, 2021; Long and Sitkin, 2018), our study illustrates emergent and unintentional aspects of control-trust dynamics. In particular, we emphasize the role of unowned processes and note the emergence of unintended control practices and trust asymmetries. Our study demonstrates that whether or not control and trust are consciously addressed, both play interacting and evolving roles in organizations. We next discuss our contributions to research on control-trust dynamics and to the specific literatures on control, and trust.

Implications for Understanding Control-Trust Dynamics

Regarding research on control-trust dynamics (Long, 2021; Long and Sitkin, 2018; Long and Weibel, 2018), our study draws attention to the role of unowned processes as well as unintended control practices and their intricate relation to developing trust asymmetries. First, it demonstrates how, depending on the trust environment, control practices may emerge unintentionally, beyond vertical or hierarchical structures, as an effect of technology deployment. Further, it illustrates how the trust implications of unintended control practices depend on the social interpretation of those practices, and how the resulting shifts in trust may, in turn, give rise to practical coping that catalyses new control practices. We suggest that looking at control-trust dynamics unfolding through unowned processes provides a possible explanation for the fact that control and trust seem sometimes irreducible (see Möllering, 2005), and at other times distinctive (see Long and Sitkin, 2006). While intentional managerial activities to build trust and control denote a separation of the two, shifting attention to unowned processes taps into more intricate control-trust dynamics, revealing their coexistence.

Second, we argue that addressing control-trust dynamics from the viewpoint of unowned processes rather than merely observing planned managerial efforts provides a more comprehensive view of the forming and re-forming of attitudes and related behaviours within organizational groups and across an organization. In particular, actions by non-managers become notably relevant to control-trust dynamics. Our study demonstrates how employees' agency goes beyond the choice to accept or decline management's control and trust-building efforts (see Gustafsson et al., 2021). A relevant example is that organizational members not only influence how distrust repair is accomplished (Brattström et al., 2019; Gillespie and Siebert, 2017; Gustafsson et al., 2021), but also initiate and independently carry out such activities (Chown, 2021) by enacting control. Considering control as a relational practice (Cooper, 2005) whereby organizational members regulate both their own behaviour and that of others in relation to organizational objectives (Delbridge and Ezzamel, 2005) offers a relevant way to understand control-trust dynamics.

A related yet distinctive insight is that once recognized, unintended control practices need to be addressed by management. At FinCo, managerial inactivity contributed to the development of suspicion and distrust when organizational members started to question the legitimacy of emergent diagonal control practices and the authority of those enacting them (DeCelles and Aquino, 2020; Piccoli and Ives, 2003; Weibel et al., 2016). Our findings caution that interpretations and effects of unintended control practices go easily unnoticed but may inadvertently change the trust environment in detrimental ways if not addressed.

Contributions to Control Research

Our consideration of unintended control effects also adds to more control-specific research. Many studies have reported that technology has spurred a shift from control based on temporal and spatial simultaneity and vertical hierarchies to horizontal, technology-enabled surveillance and monitoring (Brivot and Gendron, 2011; de Vaujany et al., 2021; Sewell and Taskin, 2015; Zuboff, 2015). Our ethnography provides a nuanced account of how unintended control practices can emerge in connection with shifts in trust. Acknowledging trust as a key aspect missing from most practice-oriented control research enables moving beyond some of the false dichotomies (Raffnsøe et al., 2019) between discipline and autonomy (de Vaujany et al., 2021), and control and freedom, that have to an extent hampered organization studies.

Another insight that our analysis brings to the literature on organizational control (Cardinal et al., 2017; Delbridge and Ezzamel, 2005; Sitkin et al., 2020) relates to the nature of control. While prior research may be seen to express negative connotations of control with pessimistic assumptions about the intent and behaviour connected both to intentional, vertical control (Sitkin et al., 2020) and its horizontal forms (Sewell and Taskin, 2015; Zuboff, 2015), our study adopts a more neutral view of control. Unintended control practices can be seen as initially neutral, engendering a broad range of possible perceptions that organizational members with different values can accept (or oppose). Hence, while formal forms of control have been considered to have limited efficiency in addressing value incongruence perceptions (Sitkin and Roth, 1993), our study suggests that in some cases their emergence may align with the expectations of those organizational members who appreciate hierarchy and formality, thereby effectively reinforcing their perceptions of value congruence.

Adding Insights into Trust

We also add to research that has shown how trust may develop or erode when changes, such as technology deployment, disrupt organizations (Bijlsma-Frankema et al., 2015; Gustafsson et al., 2021; Holland et al., 2015). Examination of the emergence of unintended control practices responds to calls for a more nuanced view of trust, distrust, and suspicion (Bijlsma-Frankema et al., 2015; Capitano and Cunningham, 2018; Zhou et al., 2017) by raising three key insights.

First, our findings provide an account of how suspicion and low levels of trust turn into distrust, locating a tipping point where concrete action – manifesting as collective resistance – was taken to counteract the vulnerability-inducing implications of the unintended organizational surveillance. In prior studies, close monitoring and surveillance have been found to generally reduce trust (Long and Weibel, 2018; Nienaber et al., 2021), and avoidance and resistance have been connected to control and surveillance on the one hand (Gabriel, 1999; Newlands, 2021) and to distrust on the other (Bijlsma-Frankema et al., 2015; Sitkin and Bijlsma-Frankema, 2018). Our study brings surveillance, resistance, and the punctuated emergence of distrust explicitly together, providing insight into the point at which suspicion or low-level trust deteriorates into distrust.

Second, connecting to previous studies that consider distrust as pervasive and escalating in self-amplifying cycles (Sitkin and Bijlsma-Frankema, 2018), our study illustrates how distrust development may be halted without specific managerial intervention. In our high-trust study context, unowned processes entailing multiple values and an acceptance that organizational members behave according to their professional roles and goals

(Rainer Jr et al., 2007) seemed to hide emerging suspicion and distrust and dampen their negative effects (Tidd et al., 2004). Negative reciprocity did not occur because the value incongruence perceptions remained one-sided and isolated (see Brattström et al., 2019) in the unowned processes.

Third, our findings provide insight into the circumstances under which distrust can be repaired and trust restored (to a low level). Prior research posits that reducing perceived value incongruence below a threshold is the key to reversing cycles of distrust (Bijlsma-Frankema et al., 2015). Our study illustrates how the process may also start from reducing vulnerability. While prior research considers avoidance to be a sign and effect of distrust (Sitkin and Bijlsma-Frankema, 2018), our findings interestingly suggest that avoidance and resistance as part of unintended control practices may signify attempts to repair distrust. We suggest that distrust can be repaired in a high-trust context when the remaining trust dimensions (in our case benevolence) are strengthened by mobilizing the core foundations of trust (Gustafsson et al., 2021) and when trustworthy managerial behaviours such as showing concern (Cui and Jiao, 2019) support this; the eroded trust elements may be addressed later.

Suggestions for Future Research

Even before the COVID-19 pandemic catapulted remote work into the public spotlight, technology had altered organizations. Our findings invite further research into several issues that arise in this newly pervasive context. We argue that unowned processes are an important aspect of control-trust dynamics and warrant closer examination. These issues may arise not only in employer-employee relations, but also between consumers and technology providers who profit from monitoring and surveillance. We also consider diagonal control a topic for future scholarly discussion. A relevant extension would be to study control practices that spread beyond organizational boundaries, both outside-in (e.g., monitoring by external service providers) and inside-out (e.g., monitoring of customers and collaborators), and how they interact with trust (and distrust). Relatedly, the question of legitimacy in relation to control-trust dynamics also requires more in-depth examination.

The limitations of our study also ground further research. First, the organization we studied was embedded in Finland's high-trust business culture, and we might expect that different control practices would emerge in a different context, so that different nuances would appear for control-trust dynamics. For example, in another context, power (e.g., Fleming and Spicer, 2014; Reed, 2001) might be a highly relevant factor to study. Second, in highlighting the views of information security experts, our analysis rests heavily on the views of organizational members who (naturally) experienced suspicion and distrust due to their training and their professional roles. While this focus provided a unique perspective on distrust development, our views of other groups' feelings were more limited and inherently influenced by the field researcher's experiences. A related, practical limitation is that not all materials could be shared among all authors. Third, as the study initially focused on information security and control-related aspects, the interviews did not include explicit questions about trust. These limitations suggest intriguing next steps for scholars studying control and trust in changing organizations. We call for more research on changes in the locus and forms of control and asymmetries of trust, as well as attention to the apparent paradoxes we observed – for example, the counterintuitive observation that information security experts responded to the availability of technological controls by limiting rather than increasing monitoring and surveillance, activities integral to their work. Acknowledging that organizations must increasingly adjust their processes to utilize information efficiently while preventing its unauthorized and inappropriate treatment, we encourage research that integrates insights from information security literature and organizational studies. We hope that our study can pave the way for these kinds of openings.

CONCLUSIONS

Prior research has accumulated extensive knowledge about the interaction of control and trust, paying attention especially to the related intentional managerial activities. Adopting a different viewpoint, we draw attention to emergence and unintentionality in control-trust dynamics. Our study outlines how deployment of new technology triggers changes in control-trust dynamics and leads to the emergence of unintended control practices. It illustrates how varying trust and control perceptions in different organizational groups shape organizational members' experiences – especially trust, suspicion, and distrust – and their actions, manifested as emerging unintended control practices. As an important insight from this study, we observe that a close interaction and coexistence of trust and control characterize the unowned processes in which unintended control practices emerge. We argue that explicit consideration of these insights offers a more comprehensive view of control and trust dynamics.

ACKNOWLEDGMENTS

We wish to express our warmest thanks to the guest editors Fabrice Lumineau, Chris P. Long, Nicholas Argyres, and especially Sim B. Sitkin, for the guidance and constructive comments. We likewise thank Professor Gideon Markman, the three anonymous reviewers, and Professor Kirsimarja Blomqvist for their feedback, though provoking questions, and insightful comments on our paper. We also value comments from participants at the special issue paper development workshop, and we extend our thanks to Rosalind Reid for her assistance in formatting, structuring, and proofreading.

NOTES

[1] These materials (recorded in Finnish) are available from the authors upon reasonable request, subject to permission from FinCo

[2] There are quotes in our material that could be said to illustrate issues of both emerging control practices and trust, suspicion, or distrust. We note here that the overlap is deliberate. Our use of the dually coded material highlights aspects of control or trust, or both (see underlined text in Tables IV and V)

REFERENCES

Aroles, J., Mitev, N. and de Vaujany, F. X. (2019). 'Mapping themes in the study of new work practices'. *New Technology, Work and Employment*, **34**, 285–99.

Ball, K. (2010). 'Workplace surveillance: an overview'. *Labor History*, **51**, 87–106.

Ball, K. and Wilson, D. C. (2000). 'Power, control and computer-based performance monitoring: repertoires, resistance and subjectivities'. *Organization Studies*, **21**, 539–65.

Bauman, Z. and Lyon, D. (2013). *Liquid Surveillance: A Conversation*. Cambridge: Polity Press.

Bernstrøm, V. H. and Svare, H. (2017). 'Significance of monitoring and control for employees' felt trust, motivation, and mastery'. *Nordic Journal of Working Life Studies*, **7**, 29–49.

Bijlsma-Frankema, K., Sitkin, S. B. and Weibel, A. (2015). 'Distrust in the balance: the emergence and development of intergroup distrust in a court of law'. *Organization Science*, **26**, 1018–39.

Brattström, A., Faems, D. and Mähring, M. (2019). 'From trust convergence to trust divergence: Trust development in conflictual interorganizational relationships'. *Organization Studies*, **40**, 1685–711.

Brivot, M. and Gendron, Y. (2011). 'Beyond panopticism: On the ramifications of surveillance in a contemporary professional setting'. *Accounting, Organizations and Society*, **36**, 135–55.

Brower, H. H., Lester, S. W., Korsgaard, M. A. and Dineen, B. R. (2009). 'A closer look at trust between managers and subordinates: Understanding the effects of both trusting and being trusted on subordinate outcomes'. *Journal of Management*, **35**, 327–47.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness'. *MIS Quarterly*, **34**, 523–48.

Capitano, J. and Cunningham, Q. W. (2018). 'Suspicion at work: The impact on counterproductive and citizenship behaviors'. *Organization Management Journal*, **15**, 174–85.

Cardinal, L. B., Kreutzer, M. and Miller, C. C. (2017). 'An aspirational view of organizational control research: Re-invigorating empirical work to better meet the challenges of 21st century organizations'. *Academy of Management Annals*, **11**, 559–92.

Chang, H., Ngunjiri, F. and Hernandez, K. A. C. (2016). *Collaborative Autoethnography*. New York: Routledge.

Chia, R. (2014). 'Reflections: in praise of silent transformation–allowing change through "letting happen"'. *Journal of Change Management*, **14**, 8–27.

Chia, R. and Holt, R. (2006). 'Strategy as practical coping: A Heideggerian perspectives'. *Organization Studies*, **27**, 635–655.

Chown, J. (2021). 'The unfolding of control mechanisms inside organizations: Pathways of customization and transmutation'. *Administrative Science Quarterly*, **66**, 711–52.

Colquitt, J. A. and Rodell, J. B. (2011). 'Justice, trust, and trustworthiness: A longitudinal analysis integrating three theoretical perspectives'. *Academy of Management Journal*, **54**, 1183–206.

Cooper, R. (2005). 'Peripheral vision: Relationality'. *Organization Studies*, **26**, 1689–710.

Costa, C. A. and Bijlsma-Frankema, K. (2007). 'Trust and control interrelations: new perspectives on the trust – control nexus'. *Group & Organization Management*, **32**, 392–406.

Cui, Y. and Jiao, H. (2019). 'Organizational justice and management trustworthiness during organizational change: Interactions of benevolence, integrity, and managerial approaches'. *Information Processing & Management*, **56**, 1526–42.

de Vaujany, F. X., Leclercq-Vandelannoitte, A., Munro, I., Nama, Y. and Holt, R. (2021). 'Control and surveillance in work practice: Cultivating paradox in "new" modes of organizing'. *Organization Studies*, **42**, 675–95.

DeCelles, K. A. and Aquino, K. (2020). 'Dark knights: when and why an employee becomes a workplace vigilante'. *Academy of Management Review*, **45**, 528–48.

Delbridge, R. and Ezzamel, M. (2005). 'The strength of difference: contemporary conceptions of control'. *Organization*, **12**, 603–18.

Den Hartog, D. N., Schippers, M. C. and Koopman, P. L. (2002). 'The impact of leader behaviour on trust in management and co-workers'. *SA Journal of Industrial Psychology*, **28**, 29–34.

Emerson, R. M., Fretz, R. I. and Shaw, L. L. (1995). *Writing Ethnographic Fieldnotes*. Chicago, IL: University of Chicago Press.

Fein, S. and Hilton, J. L. (1994). 'Judging others in the shadow of suspicion'. *Motivation and Emotion*, **18**, 167–98.

Fleming, P. and Spicer, A. (2014). 'Power in management and organization science'. *Academy of Management Annals*, **8**, 237–98.

Gabriel, Y. (1999). 'Beyond happy families: A critical reevaluation of the control-resistance-identity triangle'. *Human Relations*, **52**, 179–203.

Gillespie, N. and Siebert, S. (2017). 'Organizational trust repair'. In Searle, R., Nienenbar, A. and Sitkin ,S. (Eds), *The Routledge Companion to Trust*. London: Routledge, 284–301.

Gioia, D. A., Corley, K. G. and Hamilton, A. L. (2013). 'Seeking qualitative rigor in inductive research: Notes on the Gioia methodology'. *Organizational Research Methods*, **16**, 15–31.

Grodal, S., Anteby, M. and Holm, A. L. (2021). 'Achieving rigor in qualitative analysis: The role of active categorization in theory building'. *Academy of Management Review*, **46**, 591–612.

Guo, S. L., Lumineau, F. and Lewicki, R. J. (2015). 'Revisiting the foundations of organizational distrust'. *Foundations and Trends in Strategic Management*, **1**, 1–88.

Gustafsson, S., Gillespie, N., Searle, R., Hope Hailey, V. and Dietz, G. (2021). 'Preserving organizational trust during disruption'. *Organization Studies*, **42**, 1409–33.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J. P. (2011). 'Value conflicts for information security management'. *Journal of Strategic Information Systems*, **20**, 373–84.

Hengstler, M., Enkel, E. and Duelli, S. (2016). 'Applied artificial intelligence and trust – the case of autonomous vehicles and medical assistance devices'. *Technological Forecasting and Social Change*, **105**, 105–20.

Höddinghaus, M. and Hertel, G. (2021). 'Trust and leadership: Implications of digitization'. In Blöbaum, B. (Ed), *Trust and Communication. Findings and Implications of Trust Research*. Cham: Springer, 185–203.

Holland, P. J., Cooper, B. and Hecker, R. (2015). 'Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type'. *Personnel Review*, **44**, 161–75.

Ingold, T. (2014). 'That's enough about ethnography!' *HAU: Journal of Ethnographic Theory*, **4**, 383–95.

Janssen, M., Brousa, P., Estevez, E., Barbosad, L. S. and Janowski, T. (2020). 'Data governance: organizing data for trustworthy Artificial Intelligence'. *Government Information Quarterly*, **37**, 101493. https://doi.org/10.1016/j.giq.2020.101493.

Järventie-Thesleff, R., Logemann, M., Piekkari, R. and Tienari, J. (2016). 'Roles and identity work in "at-home" ethnography'. *Journal of Organizational Ethnography*, **5**, 235–57.

Jarzabkowski, P., Bednarek, R. and Cabantous, L. (2015). 'Conducting global team-based ethnography: Methodological challenges and practical methods'. *Human Relations*, **68**, 3–33.

Langley, A. (1999). 'Strategies for theorizing from process data'. *Academy of Management Review*, **24**, 691–710.

Langley, A., Smallman, C., Tsoukas, H. and Van de Ven, A. H. (2013). 'Process studies of change in organization and management: Unveiling temporality, activity, and flow'. *Academy of Management Journal*, **56**, 1–13.

Lessig, L. (2006). *Code. And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books.

Lines, R., Selart, M., Espedal, B. and Johansen, S. T. (2005). 'The production of trust during organizational change'. *Journal of Change Management*, **5**, 221–45.

Long, C. P. (2018). 'To control and build trust: how managers use organizational controls and trust-building activities to motivate subordinate cooperation'. *Accounting, Organizations and Society*, **70**, 69–91.

Long, C. (2021). 'Cascading influences and contextualized effects'. In Gillespie, N., Fulmer, C. A. and Lewicki, R. J. (Eds), *Understanding Trust in Organizations: A Multilevel Perspective*. New York: Routledge.

Long, C. P. and Sitkin, S. B. (2006). 'Trust in the balance: How managers integrate trust-building and task control'. In Bachmann, R. and Zaheer, A. (Eds), *Handbook of Trust Research*. Cheltenham: Edward Elgar Publishing Limited, 87–106.

Long, C. P. and Sitkin, S. B. (2018). 'Control–trust dynamics in organizations: Identifying shared perspectives and charting conceptual fault lines'. *Academy of Management Annals*, **12**, 725–51.

Long, C. P. and Weibel, A. (2018). 'Two sides of an important coin: Outlining the general parameters of control-trust research'. In Searle, R. H., Nienaber, A.-M. I. and Sitkin, S. B. (Eds), *The Routledge Companion to Trust*. London: Routledge, 506–21.

Loughry, M. L. and Tosi, H. L. (2008). 'Performance implications of peer monitoring'. *Organization Science*, **19**, 876–90.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

MacKay, R. B. and Chia, R. (2013). 'Choice, change, and unintended consequences in strategic change: A process understanding of the rise and fall of Northco Automotive'. *Academy of Management Journal*, **56**, 208–30.

Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995). 'An integrative model of organizational trust'. *Academy of Management Review*, **20**, 709–34.

Mcknight, D. H., Carter, M., Thatcher, J. B. and Clay, P. F. (2011). 'Trust in a specific technology: An investigation of its components and measures'. *ACM Transactions on Management Information Systems*, **2**, 1–25.

Möllering, G. (2005). 'The trust/control duality: An integrative perspective on positive expectations of others'. *International Sociology*, **20**, 283–305.

Newlands, G. (2021). 'Algorithmic surveillance in the gig economy: The organization of work through Lefebvrian conceived space'. *Organization Studies*, **42**, 719–37.

Nicolini, D. (2009). 'Zooming in and out: Studying practices by switching theoretical lenses and trailing connections'. *Organization Studies*, **30**, 1391–418.

Nienaber, A. M., Spundflasch, S., Soares, A. and Woodcock, A. (2021). 'Distrust as a hazard for future sustainable mobility planning. Rethinking employees' vulnerability when introducing new information and communication technologies in local authorities'. *International Journal of Human – Computer Interaction*, **37**, 390–401.

Piccoli, G. and Ives, B. (2003). 'Trust and the unintended effects of behavior control in virtual teams'. *MIS Quarterly*, **27**, 365–95.

Puranam, P., Alexy, O. and Reitzig, M. (2014). 'What's "new" about new forms of organizing?'. *Academy of Management Review*, **39**, 162–80.

Raffnsøe, S., Mennicken, A. and Miller, P. (2019). 'The Foucault effect in organization studies'. *Organization Studies*, **40**, 155–82.

Rainer, R. K., Jr., Marshall, T. E., Knapp, K. J. and Montgomery, G. H. (2007). 'Do information security professionals and business managers view information security issues differently?' *Information Systems Security*, **16**, 100–08.

Reed, M. I. (2001). 'Organization, trust and control: A realist analysis'. *Organization Studies*, **22**, 201–28.

Rousseau, D. M., Sitkin, S. B., Burt, R. S. and Camerer, C. (1998). 'Not so different after all: A cross-discipline view of trust''. *Academy of Management Review*, **23**, 393–404.

Sandberg, J. and Tsoukas, H. (2011). 'Grasping the logic of practice: Theorizing through practical rationality'. *Academy of Management Review*, **36**, 338–60.

Schultze, U. (2000). 'A confessional account of an ethnography about knowledge work'. *MIS Quarterly*, **24**, 3–41.

Searle, R., Den Hartog, D. N., Weibel, A., Gillespie, N., Six, F., Hatzakis, T. and Skinner, D. (2011). 'Trust in the employer: The role of high-involvement work practices and procedural justice in European organizations'. *The International Journal of Human Resource Management*, **22**, 1069–92.

Sewell, G. (1998). 'The discipline of teams: The control of team-based industrial work through electronic and peer surveillance'. *Administrative Science Quarterly*, **43**, 397–428.

Sewell, G. and Taskin, L. (2015). 'Out of sight, out of mind in a new world of work? Autonomy, control, and spatiotemporal scaling in telework'. *Organization Studies*, **36**, 1507–29.

Simons, R. (1994). *Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal*. Boston, MA: Harvard Business Press.

Sitkin, S. B. and Bijlsma-Frankema, K. M. (2018). 'Distrust'. In Searle, R. H., Nienaber, A.-M. I. and Sitkin, S. B. (Eds), *The Routledge Companion to Trust*. London: Routledge, 50–61.

Sitkin, S. B. and Roth, N. (1993). 'Explaining the limited effectiveness of legalistic "remedies" for trust/distrust'. *Organization Science*, **4**, 367–92.

Sitkin, S. B., Long, C. P. and Cardinal, L. B. (2020). 'Assessing the control literature: Looking back and looking forward'. *Annual Review of Organizational Psychology and Organizational Behavior*, **7**, 339–68.

Sørensen, O. H., Hasle, P. and Pejtersen, J. H. (2011). 'Trust relations in management of change'. *Scandinavian Journal of Management*, **27**, 405–17.

Stanton, J. M. (2000). 'Reactions to employee performance monitoring: Framework, review, and research directions'. *Human Performance*, **13**, 85–113.

Stieninger, M., Nedbal, D., Wetzlinger, W., Wagner, G. and Erskine, M. A. (2014). 'Impacts on the organizational adoption of cloud computing: A reconceptualization of influencing factors'. *Procedia Technology*, **16**, 85–93.

Thielsch, M. T., Meeßen, S. M. and Hertel, G. (2018). 'Trust and distrust in information systems at the workplace'. *PeerJ*, **6**, e5483.

Tidd, S. T., McIntyre, H. H. and Friedman, R. A. (2004). 'The importance of role ambiguity and trust in conflict perception: Unpacking the task conflict to relationship conflict linkage'. *International Journal of Conflict Management*, **15**, 364–80.

van Hulst, M. J. (2008). 'Quite an experience: Using ethnography to study local government'. *Critical Policy Analysis*, **2**, 143–59.

van Hulst, M., Ybema, S. and Yanow, D. (2017). 'Ethnography and organizational processes'. In Langley A. and Tsoukas, H. (Eds), *The SAGE Handbook of Process Organization Studies*. London: Sage, 223–36.

Weibel, A., Den Hartog, D. N., Gillespie, N., Searle, R., Six, F. and Skinner, D. (2016). 'How do controls impact employee trust in the employer?' *Human Resource Management*, **55**, 437–62.

Whitener, E. M., Brodt, S. E., Korsgaard, M. A. and Werner, J. M. (1998). 'Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior'. *Academy of Management Review*, **23**, 513–30.

Zhou, X., Liao, J. Q., Liu, Y. and Liao, S. (2017). 'Leader impression management and employee voice behavior: Trust and suspicion as mediators'. *Social Behavior and Personality: An International Journal*, **45**, 1843–54.

Zuboff, S. (2015). 'Big other: Surveillance capitalism and the prospects of an information civilization'. *Journal of Information Technology*, **30**, 75–89.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books Ltd.

APPENDIX
DESCRIPTION OF THE EMPIRICAL MATERIAL

Type of material collection	*Material collection activity*	*Time span of material collection*	*Description of the material and type of information provided*	*Quality of the evidence*	*Limitations of the material*
Field notes about informal occasions (meetings, lunch and coffee break discussions etc.) and ebb and flow of organizational life	Auto-ethnography Field researcher working as an information security expert	Jan 2016 – Dec 2017; Additional visits 2018 and 2019 • Main events on technology deployment from Nov 2016 – Jun 2017; The other times focus more on information security policy and do not depict control or trust-related issues The wider materials served as familiarization needed for collecting ethnographic material (see van Hulst, 2008)	Field notes (field note template mode by Schultze (2000)) including date, location, main events, small/odd events, main actors, a description of the day, and early interpretation and personal notes. • 128 pages of field notes (including 30 pages of non-confidential notes on new technology deployment between Nov 2016 – Jun 2017) that include: • *Observation notes* that cover direct observation of the organizational actors, their actions, and speech. Approximately 75% of the field notes • *Field researcher's personal notes* that focus on researcher's own feelings and perceptions of varying situations (including documented interpretation of the situation by the field researcher) written onsite either real-time or shortly after. Approximately 25% of the field notes.	+++	Confidential parts coded and analysed only by the field researcher; Early and late materials have only limited insight into the technology, trust, or control practices
Observation of official meetings and workshops	Participant observation –Meeting	Nov 2016	Information security status check • Information on the initial situation	++	Confidential parts coded and analysed by the field researcher alone
	Participant observation –Meeting	Jan 2017	Renewal of organization intranet • First indications of change related to O365	++	
	Participant observation –Meeting	Feb 2017	Information security status check • First indications of changing practices	++	
	Participant observation –Meeting and workshop	Mar 2017	Features of the new technology introduced by IT experts • Information on the technology features • Information on the level of IT knowledgeability • Indications of suspicion arising among InfoSec experts	+++	
	Participant observation –Meeting	May 2017	Information security status check • Indications of activities toward repairing distrust	++	
	Participant observation –Meeting	June 2017	Information security status check • Proposal to deepen employee monitoring refused by InfoSec experts	++	
	Participant observation –Workshop	June 2017	Planning for new solutions to monitor and prevent information leaks • Indications about the need to control the sharing of confidential information in an appropriate manner	++	

Type of material collection	*Material collection activity*	*Time span of material collection*	*Description of the material and type of information provided*	*Quality of the evidence*	*Limitations of the material*
Interviews (with 22 individuals) Recorded and transcribed *in verbatim*	Group interview –Two information security experts	March 2017	• Views on the control-enabling features of the new technology • Control practices adopted by the employees • Emerging privacy concerns	+++	Second-hand knowledge of control practices; implicit references to trust
	Group interview – Four financial professionals	March 2017	• Views on the new technology and work practices allowed by it • Views on information security features from the employee perspective	++	Possible domination by individual interviewee; implicit references to trust
	Group interview – Two financial professionals	March 2017	• Views on the new technology and work practices allowed by it • Views on security features from the employee perspective	++	Confidential parts coded and analysed by the field researcher alone; implicit references to trust
	Group interview – Three service-level employees	March 2017	• Views on the new technology and work practices allowed by it	+	Interviewees seemed to have a hard time understanding the topic
	Group interview – Two legal experts	March 2017	• Views on the new technology and work practices allowed by it • Views on information security features from the employee perspective	++	Confidential parts coded and analysed only by field researcher; implicit references to trust
	Group interview – Four service-level employees	March 2017	• Views on the new technology and work practices allowed by it • Views on information security features from the employee perspective	+	Interviewees seemed to have a hard time understanding the topic
	Group interview – Three financial professionals	March 2017	• Views on the new technology and work practices allowed by it • Views on information security features from the employee perspective	++	Confidential parts coded and analysed by the field researcher alone; implicit references to trust
	Interview – Risk management director	April 2017	• Views on the new technology and work practices allowed by it allows; related risks • Views on information security features from the management perspective	++	Confidential parts coded and analysed only by the field researcher alone; implicit references to trust
	Interview – Director of human resources	May 2017	• Views on the new technology and work practices allowed by it; related risks from the management perspective	++	Confidential parts coded and analysed by the field researcher alone

Note: +++ = Extensive material that covers a long time period or material that extensively captures the views of numerous groups and/or the interviewed persons and the groups they represent

++ = Material that covers a short time period (e.g., one meeting) or material that shows the views of limited groups and/or partially illustrates the views of the interviewed persons and the groups they represent.

+ = Material that covers a short time period (e.g., one meeting) or material that provides limited views of the interviewed persons and the groups they represent (e.g., there is uncertainty regarding whether interviewees have understood the questions accurately or responded comprehensively).