
Article:
Prentice, M.M. orcid.org/0000-0003-2981-7850 (2021) The securitized workplace : document protection, insider threats and emerging ethnographic barriers in a South Korean organization. Journal of Organizational Ethnography, 10 (3). pp. 258-273. ISSN 2046-6749

https://doi.org/10.1108/JOE-02-2021-0010

The securitized workplace: document protection, insider threats and emerging ethnographic barriers in a South Korean organization

Michael M. Prentice

Journal of Organizational Ethnography

Abstract

Purpose

The purpose of this paper is to demonstrate how document protection has become a key object of concern for organizations, how the threat of leaks has led to an increase in security technologies and policies and how these developments present new and emergent ethnographic challenges for researchers. Through a study of a South Korean organization, the paper aims to demonstrate the ways workplace documents are figured into wider legal, regulatory and cyber security concerns.

Design/methodology/approach

The research is based on 12 months of intensive embedded fieldwork in a South Korean firm from 2014 to 2015 and follow-up interviews in 2018. The author followed an immersive and inductive approach to collecting ethnographic data in situ. The author was hired as an intern in a Korean conglomerate known as the Sangdo Group where he worked alongside Human Resources managers to understand their work practices. The present article reflects difficulties in his original research design and an attempt to analyze the barriers themselves. His analysis combines ideas from theories of securitization and document studies to understand how the idea of protection is reshaping workplaces in South Korea and elsewhere.

Findings

The paper highlights three findings first that South Korean workplaces have robust socio-material infrastructures around document protection and security, reflecting that security around document leaks is becoming integrated into normal organizational life. Second, the securitization of document leaks is shifting from treating document leaks as a threat to organizational existence, to a crime by individual actors that organizations track. Third, that even potential document leaks can have transitive effects on teams and managers.

Originality/value

Organizational security practices and their integration into workplace life have rarely been examined together. This paper connects Weber's insights on bureaucratization with the concept of securitization to examine the rise of document security practices and policies in a South Korean organization. The evidence from South Korea is valuable because technological developments around security coupled with organizational complexities portend issues for other organizational environments around the world.

Introduction

As high-profile leaks of corporate and government information from Wikileaks to the Panama Papers attest, documents have become a key medium through which publics can pierce the figurative veil of large corporations, government actors and other organizations. Such leaks appear to confirm conventional notions of organizations and government bodies as singular, enclosed entities for whom the loss of documents represents a significant harm. This goes against a broad set of literature in organization studies that has long shown that organizations and organizational boundaries are layered, porous, overlapping, competing, contingent and fuzzy in practice (Paulsen and Hernes, 2003; Dahles and Leng, 2005; Czarniawska, 2008; Scott and Davis, 2007). Indeed, organizational researchers have long been skeptical of formal, reified accounts of organizations (Bittner, 1965), yet corporate espionage, data regulations and cyberattacks, alongside the continued reliance on documents, the rise of digital text production and information/data hoarding, have nevertheless helped to reinforce the idea of an inside–outside distinction [1].

Ethnographers are keenly aware of the difficulty accessing such "inside" locations poses. For anthropologists, gaining inside access has often been understood as a social problem, such as accessing the worlds of elites, powerful economic actors or auratic institutions like Hollywood (Gusterson, 1997; Ortner, 2010; Souleles, 2018; see also Seaver, 2017), under the assumption that such actors do not want to be studied and are protecting their own secretive spaces from outsiders. Anthropologists have found ways of working around these constraints through creative ethnographic methods, such as Garsten's (2010) and Ortner's (2010) notions of "interface" ethnography. These are important for demystifying the "inside" as a special or necessary zone of action that ethnographers must reach to study powerful actors or institutions (see Monahan and Fisher, 2015). However, in the search for new and alternative methods outside the organization, the question of why internal access for ethnographic research is (ever more) closed off to the ethnographer has not been readily explored. Rather than seeing employees, elites or organizations as the eternal gatekeepers (or gateclosers) that prevent access to outsiders, this article foregrounds how security concerns around document leaks and document protection are mediating questions of access.

As the global interest in leaks and cyberattacks suggests, written documents have become one of the key objects of security concerns, particularly in white-collar organizations, where records, reports, emails, contracts and a host of other inside written genres form a quasi-protected class of artifacts. Where documents have long been treated as an object of office floor practice and sense-making in organizations (see Garfinkel, 1967, pp. 186–207), I foreground the ways that the document leak has become a zone of organizational threat and risk. Through an "insider" ethnography of a South Korean corporate organization called Sangdo and more general descriptions of document security in South Korea, I describe how concerns over document protection spread across different socio-technical modalities, including legal agreements, digital scanning devices, physical infrastructures and normative concerns among co-workers.

A concern for document protection (if not documents per se) is undergoing what Weber would have described as an effect of bureaucratization: the "concentration of the material means of management in the hands of the master" (1978, p. 850). This is to say that documents are not just an instrument of bureaucracy, but now a concern of it, particularly their form, storage and ownership. This is significant not only because it represents another frontier of bureaucratic creep, but because it contributes to what Weber described as "the

"separation" of the administrative staff. . .of officials and employees, from the material resources of administration," or (borrowing Marx's phrase) "the expropriation of the expropriator" (Weber, 2004, p. 38). In other words, such a move has started to delineate organizational insiders from the organizational inside. Documents, as I will discuss, are increasingly becoming preserved within organizations, but are also being separated from those we might imagine as the preservationists. This is particularly evident amidst new narratives and expertise around "insider threats." Insider threat discourse has problematized employees as individuals who, due to bad intentions, stress, or carelessness, cause potential harm to their organizations by allowing outsiders to access, ransom or damage inside "property" [2]. These narratives (alongside new cyber security projects and data regulations) have naturalized the idea of data and documents as basic units of property that must be kept "within" an organization.

In this sense, workplaces are increasingly become securitized. By securitized, I draw on the concept of "securitization" which was originally developed by critical international relations scholars (Buzan et al., 1998; McDonald, 2008) and which captures the way that certain kinds of people, groups or objects become discursively framed as threats to a national or international order in order to legitimize exceptional, protective measures against them. While more commonly used to critique threats to global peace posed by non-conforming nations or panics of mass migration which seem to "threaten" domestic polities, the concept is useful for understanding, and critiquing, the spread of security narratives, technologies and policies within organizations. Here, exfiltration or loss of documents constitutes an existential threat to an organization, motivating various "securitizing moves" such as instituting multi-factor encryption and new document security protocol. In this article, I describe increasing sociotechnical efforts in South Korea to hyper-protect organizational documents as well as security norms around the protection of documents as new benchmarks for employee (mis)behavior. Behind, surrounding, and shaping everyday office practices and workplaces lies a complex assemblage of apparati.

In my analysis of ethnographic data from South Korea, I suggest that such securitization is making workplaces new "spaces of security" (Maguire and Low, 2019). One of the effects of this is increasingly treating employees, including higher-level managers, as quasi-outsiders vis-_a-vis documents. That is, as documents become seen as a kind of property that belongs in the office, employees become relegated to "users" with "access" to such material rather as trusted guardians of it themselves. For ethnographers, this trend shifts the understanding of "access" itself, as it becomes premised not solely on access to people or spaces through good ethnographic knowhow, but on access to people who have certain kinds of access to documents in certain kinds of spaces. Ethnographers may find formal employment organizations even more difficult to access as a result, but it also has implications for what we consider an organizational insider, in an era when employment might be understood less around organizational roles (the purely social), and more on models derived from legal and IT (the social in relation to material/digital property).

My analysis is based on embedded participant observation at the "Sangdo Group," a pseudonym for a large South Korean industrial conglomerate. My research with Sangdo entailed working as an intern in the headquarters for a period of one year in 2014–2015 while being allowed to conduct daily observations and both formal and informal interviews with white-collar employees, managers and executives. I was also able to speak to some former employees for informal follow-up interviews in 2018. My initial ethnographic goal was to

look at the relationship between office democratization discourses and genres of work among white-collar workers in South Korea. Methodologically, I intended to gather and analyze different genres and practices (meetings, emails, intranets, document-writing and so on) within teams across one organization, in the spirit of research on genres of management (e.g. Yates, 1989; Turco, 2016) [3]. Even though I was permitted to conduct research internally through my role as an intern working at the headquarters and had ample social access to different employees to shadow, interview or develop informant-like relationships, I also encountered visible and invisible barriers to accessing and analyzing documents or other written or digital artifacts. For example, though I often asked my coworkers in Human Resources about different genres I was interested in, like emails, memos or formal reports, they were often reluctant to give me examples or photo-copies. Nominally an "insider" on the team, they did not alert me to the presence of digital files commonly used by other members of the team until near the end of my fieldwork. As an official "intern", I found myself often at the fringe (or bottom rung) of internal document visibility,with access to company magazines, generic announcements on the intranet, internal websites, document templates and low-level projects I worked on. When I ended my formal research with Sangdo in 2015 and left Seoul, I felt disappointed due to the lack of access to the kinds of knowledge embedded in documents I knew existed and thought would be necessary for my dissertation. I initially thought this lack of access represented my coworkers' silent disavowal of my research (despite our year working side-by-side). In hindsight, I have come to see their actions as part of a broader concern around document security, which increasingly entangled them in complex forms of responsibility.

Following an anthropological tendency to use such barriers as ethnographic facts in and of themselves, I revisited my original ethnographic fieldnotes and conducted extra interviews on a return visit to the company in 2018 in the development of this article. Though much of my original data reflected concerns about new ideas about equality, merit and two-way communication in the South Korean workplace, other aspects of my notes and discussions with employees reflected a high degree of concern and awareness for document security measures, as well as conflicts between managerial expectations of authority and emerging IT controls.

South Korea offers a privileged position from which to understand the shifting dynamics of documentation and security. On one side, the South Korean economy is still dominated by large conglomerates, known as daegieop, inclusive of what are often referred to as "chaebol" in international management [4]. As conglomerates, such organizations are intersected by complex financial ties, shared production and operations, and management hierarchies across many subsidiaries. Their outwardly unified image (such as Samsung Electronics, Samsung Heavy Industries, Samsung Life Insurance) is undercut by a vast array of competing administrative systems and hierarchies that span multiple subsidiaries. These administrative systems are mediated by an array of forms, reports and planning genres that intersect and complicate working life. It is not uncommon for South Korean office workers to describe their work derogatively as "bureaucratic" (*gwallyojeok*) based on the time spent writing reports. On the other side, South Korea represents an interesting case from the point of view of a robust digital infrastructure: the country has one of the highest broadband and smartphone penetration rates in the world spurred by pro-active government policies since the late 1990s that have promoted digitization of services at national and local levels (Jin, 2017; Yang, 2017). Alongside this, South Korea was one of the first countries to implement robust

digital security protocol in the form of public-key infrastructure beginning in the late 1990s (Park, 2015).

In what follows, I first situate the article in the context of scholarship on documents and securitization to suggest that documents have become a key material artifact through which new organizational security concerns have become concentrated. Turning to the Korean case, I describe how organizational documents exist in a wider economy of leaks in relation to public transparency and exposure in South Korea. Elements of document security and control are inscribed into various technologies, formal policies and informal practices in corporate office spaces and concern over leaks is increasingly leading to an individualization of threats. In the final section, I describe two periods of time at Sangdo: during my research in 2014–2015, document security measures were commonplace, but managers had their own authority to handle team-level and individual document security. When I returned in 2018, employees described a new cloud-based encryption system that had greatly affected their working relations by encrypting every digital document and increasing internal surveillance of document movement. In the conclusion, I suggest how securitization complicates ethnographic research encounters in organizations and how ethnographers can work within such constraints.

Documents and securitization of the firm

Weber famously described bureaucracy in relation to documents. "Management of modern offices," he wrote, "is based on written documents (the files)which are preserved in theirwritten or draft form" (Weber, 1978, p. 957, emphasis added). Yet the relationship between documents and their "preservation" within bureaucratic organizations (including corporations) has remained largely a functional one. In one of the few studies of the history of document storage, Yates (1982) described the advent of vertical filing cabinets in relation to the need to preserve organizational memory in the early twentieth century American corporation. The proliferation of cloud storage services, worries that corporations hoard documents and data, and new discussions of data sovereignty, suggest that the preservation of documents has become less a functional necessity to access documents quickly and more associated with fear of attack and exposure to outsiders. Situating these concerns within a longer perspective on capitalism, media theorist Lisa Gitelman understands documentation itself as a kind of enclosure movement. She has described the continued refinement of documentation techniques into the twenty-first century as an articulation of the "micrologics of enclosure and attachment" (Gitelman, 2014, p. 32) – that is, an attempt to enclose and contain content in a material form, especially as documents move within and across organizational spaces. These "micrologics" are visible in the rise of physical efforts to store and copy documents in archives, legal efforts to attach copyrights and digital efforts to reproduce the same text anytime, anywhere and in any format [5].

Today, with the exception perhaps of radically transparent organizations, it is largely axiomatic that companies or organizations do not reveal their information to outsiders, particularly written or digital documents. It is indeed quite rare that the public even encounters organizational documents. There are legal and regulatory reasons for this, such as the protection of personally identifying information and concerns over intellectual property. But another reason is the counter-effect of transparency discourses over the latter half of the twentieth century: transparency movements, driven by an ideology of communication associating documents with knowledge, and possession with control, have led to more

concern about leaks, and greater concern over information enclosure in turn (Fenster, 2005, 2015) [6]. There are many classes and genres of documents that have little value to organizational information, such as sticky notes, records, drafts of PowerPoint slides or internal message boards, that also become wrapped up in such concerns. Indeed, there has been only one large-scale email corpus made available from an actual company – the Enron corpus (see Diesner et al., 2005) – that has become published as part of organizational analysis, reflecting that it is accepted among academic researchers and publishers alike to treat documents as proprietary objects [7].

Such securitization could be understood as a new kind of workplace surveillance, but organizational actors also become involved in workplace security. In their research on "security in the wild," Dourish et al. (2004) discussed how staff at a research lab did things that seemed to overelaborate organizational security practices in ways not formally mandated, such as including notices about legal and illegal use of attachments at the bottom of their emails, or covering their screens with paper to prevent others from seeing information when they left their desks (p, 396). In South Korea, employee access cards, a basic security device, have become fashion-like status items, with one's headshot, name, corporation and sometimes department visibly displayed which most employees wear on a lanyard all day long. More generally, anthropologist Schull (2018) has described new moral discourses emerging around digital information storage. Individuals in digital societies, she notes, are increasingly being asked to monitor their own data and to make sure that one's "self-data" are properly contained, protected and tracked. These practices reflect the fact that organizational security is no longer a fact decided by the organization through basic secrecy levels or access controls (Gusterson, 1996, pp. 68–100; Yost, 2015). Security is co-produced by employees, a fact reinforced in digitally managed personal lives. The variety of different adaptations to security, sometimes going above and beyond what is required, is suggestive of the ways that employees have some authority in enacting security and protection based on their own knowledge and familiarity with their environments. In this sense, even in a regime in which they are protecting documents as property, they are also enrolled and delegated as guardians too. It is precisely this understanding that began to cleave during and after my fieldwork at Sangdo. I first turn to describing a more general context of leaks in South Korea.

An economy of leaks

Concerns over the misappropriation of company information and documents are a persistent feature of headlines in South Korea. Former President Park Geun-hye was removed from office in 2017 after a neglected tablet was uncovered by a journalist and contained copyedited drafts of presidential speeches made by an unofficial consigliere figure, Choi Soon-sil. More generally, public transparency relies on public fact-finding through revealed or misplaced documents that seem to confirm insider secrets [8]. One of the most common forms of public gossip is known as *jjirasi*, short messages containing salacious gossip about politicians and celebrities that circulate by mobile phone. In corporate circles, "securities jjirasi" (*jeung-kwon jjirasi*) are reports containing insider and advanced information on corporate news and scandals the aim of which is to alter stock prices. And among corporate groups, there is a notion that some offices hoard documents more than others: the Samsung Group, for instance, was revealed in 2005 to have its own secret archive of secret documents known as the "X-files" (x pail) that was reputed to be more thorough than the Korean CIA's and through which they could strategically leak private information about those who criticized the conglomerate.

In South Korea, leaks can and do have consequences. In corporations, employees can abscond to competitors in tightly competitive industries. And in regulatory audits, prosecutors, tax officials or police can conduct raids on large corporate groups, carrying out boxes of paper documents to be photographed by the press as a sign of "checking the books." While conducting research at the Sangdo Group, I learned of one subsidiary which faced an unexpected tax raid in which government investigators came into the office and extracted digital files from every computer in the office via specially made USB keys. Public investigations of internal dealings can lead to fines, public scrutiny or increased regulatory oversight. And sensitive information related to owners' activities can lead to reputational damage. These acts nevertheless undergird the idea that files, both digital and paper, are the objective source of such secrets and thus act as a kind of valued, internal property that bear important information on privileged actors, regardless of whether they contain anything of informational value.

Within such a context, large corporate office towers in Korea act as veritable fortresses. For visitors, portable storage devices are temporally confiscated, disabled or logged in a book. Smartphone cameras are taped over to prevent photographic theft of documents. The same mechanisms apply as much to employees: employee bags can be scanned on their way out of work, local storage on hard drives can be automatically erased every night and IT departments can monitor what is written on emails or documents. One interviewee I spoke to at a large conglomerate mentioned their company had remote software that could disable employees' mobile phone cameras and audio-recording simply when they entered the building. Another noted that their IT departments scanned internal documents and emails that mentioned the word "chairman" (hoejang) for potential gossip leaks. Because of these security concerns, I never saw employees work on documents on the train or subway, or even take physical paper home, even in briefcases. As such, working from home for corporate employees was largely an anomaly in (pre-pandemic) South Korea. The tethering of documents to office spaces was one reason Korean white-collar employees spent so much time at work.

Concerns over document leaks are of course not unique to South Korea, and even within the country there are vast differences in policies across companies. I highlight however the degree to which the securitization of document leaks manifested in an array of social and material modalities for protection, based on my ethnographic observations at Sangdo. At the time, the group did not have high-tech document protection systems, but did have other mechanisms, such as conventional document classifications delineating possible arenas of circulation. These included stamps and graphics saying "outside-forbidden" (*daeoebi*) as well as "outside-inside forbidden" (*daenaeoebi*) for higher status documents that were not to circulate internally. Such classifications could be placed at the top of emails or internal memos and physically stamped onto a cover page. Furthermore, employees at Sangdo had to sign legal statements at the beginning and end of their employment attesting that they would not take (or had not taken) any company documents from their place of work. At the beginning of a calendar year, all employees had to re-sign "ethical management pledges" (*yulli gyeongyeong silcheon seoyakseo*) which they signed to aver they would not conduct any unethical business involving bribery or private dealing. Employees also had to agree to more detailed "information protection agreements" (*jeongbobohoui dong-uiseo*) in which they attested that they would protect company important secrets and related industrial information to the best of their abilities, as well as pledge to not reveal or take information

when they left the company, and to report anyone who did so. (In the case of human resources information, the exfiltration of personnel data could generate a government fine for loss of personally identifiable information). For information related to operations, I had heard indirectly of instances in which the company's auditing department itself sued individual employees who were found to have taken manufacturing or sales information when they left the Sangdo Group (though not necessarily between subsidiary companies) [9]. And before I left the company, the Auditing department was working on implementing a "real-time monitoring" (*sangsi monitoring*) system. Such a digital system, integrated into the shared group intranet, could allow them to track document uploads and movement across the entire conglomerate in a way that they could not previously.

Some of the social and technological build-up of security efforts at Sangdo reflects legal and regulatory concerns toward organizational culpability; other facets however point to attempts to link documents to specific people. An IT manager at Sangdo relayed a story along these lines. According to him, the executives at one subsidiary had requested the IT manager's team to modify the printer software so that employee names would appear on the bottom edge of every page as they had become concerned about leaks from their office. This would in theory preserve the image of a document without interfering in its visual display, while keeping a traceable record of who printed it. Later, the executives found out that employees could simply cut off the bottom edge to hide their names. Management then asked the IT department to change the printer again so that the employee's name, their department, the date and the time would be printed diagonally across the middle of a document like a watermark, thereby making the person who printed it (not necessarily the author) inseparable from the content. My co-workers in the headquarters (with their unwatermarked documents) thought this practice to be quite an extreme response. They were surprised when a few years later it was mandated that their own documents also be printed in this way [10]. If that anecdote represents a mode of closely tying individuals to documents, popular representation of office dynamics demonstrates high concern for individual conduct around documents as well. There is a tense sequence in the widely popular Korean television drama (based on a graphic novel) Misaeng, or "An Incomplete Life," that illustrates this. In the scene, an intern at the fictitious firm One International unwittingly picks up a sales proposal from a pile of documents that was meant to be shredded. In his rush to a meeting, the intern realizes his mistake and leaves the document on the lobby counter for a company security guard to dispose. The document slips to the floor where it is discovered by none other than a high-ranking One International executive. Reading its source, the executive takes the proposal back to the sales team, where he rebukes the team's manager for being careless with company information by allowing a company document to escape its office home. Once the executive leaves, the team manager and an assistant manager proceed to scold their junior team member who was supposed to have shredded the proposal. The junior team member, unaware of the intern's mistake, is dumbfounded by how it got to the lobby in the first place. He nevertheless accepts blame for the mistake. This scene from the show (which was frequently discussed in the Sangdo office while it aired) reflects the way that individuals can become conditionally responsible for documents of which they are not authors and how this responsibility is tied to the individual reputations of others.

I realized how seriously employees were aware of potential responsibility for retro-active leaks after I defended my dissertation in 2017. When I shared my dissertation electronically with some employees at Sangdo as a token thank you for their cooperation (two

years after leaving the company and South Korea), one manager replied to me with a request to correct part of my dissertation that he believed was in error: a mention I had made (even with a few degrees of anonymization) of using a hard drive of files from a previous company as reference in his current work; he made no other comment about the dissertation. Even though the files were not from his current role, there was nevertheless a concern, I suspected, of a kind of second-order caution being represented on paper. That is, he did not want to be seen as someone who might take documents from job to job, especially if other members of Sangdo were to read the dissertation (in English no less). This confirmed another retrospective observation during my time at the company in 2014–2015: any document I came to observe or store on my work computer was either previously accessible or part of a finite work project. My requests to employees of genre examples that I could use in my study (e.g. a spreadsheets, PowerPoints or emails) were usually met with no responses or offers for quick "walk-throughs" on their own screens [11]. It is of course entirely reasonable that employees would not want to share documents arbitrarily to a temporary foreigner-interloper like myself; however, where a common answer might be that secrecy was a core part of their "group-ness" (in Simmelian fashion), I suggest that part of it has to do with such second-order concerns around document leaks and perceived harm to their organization, and perhaps from it as well. As I describe in the next section, Sangdo employees were socialized to be highly aware of document protection.

From guardians to threats

When I was embedded with an HR department at a Sangdo subsidiary for a few weeks during my research, I helped members of HR clear old documents from a closet to take to a shredder. Some of the employees discovered a pile of English-language test score results from the mid- 1990s. The documents, which had been produced on an older style of computer paper and had become discolored over time, contained a long list of names and numerical test results. Given they were headed for the shredder and involved employees long gone, I thought they might prove valuable for comparison with modern contemporary document formats. I asked a few junior employees if I could hold onto a few as a sample which they thought was fine. As I was looking over them at a desk, a senior HR manager came over, grabbed the pile from my desk and tossed them into a plastic bag to be shredded. The senior manager did not offer any verbal reason for doing so, but the message was clear that I was not to siphon off such documents, even for perusal. In a similar incident, during a small project I was working on in the headquarters HR team, a junior manager told me about a shared server that the team used to share and store digital files for team projects. Despite being an intern-researcher on that team for around eight months and being an insider with them in many other senses, I had not known about the server's existence nor the files stored on it. To my surprise, I found a neatly organized server containing all the team's projects for that year and years prior. When I finished a draft of the report for the project, I emailed a senior HR manager to let him know that I had uploaded it to this server for his review. The next day the senior HR manager sequestered two HR employees one-on-one in back-to-back meetings in a small meeting room. After meeting both, he called me in to tell me he had been concerned with how I had gotten access to the server and that he had been interrogating his two subordinates to trace the process. His concern, overlooked by one of the junior managers at the time, was that my access to the server meant that I would be able to see too many of the headquarters HR department documents, including certain documents related to promotions,

especially their drafts and revisions. He was overtly concerned with a moral hazard: I, the unwitting ethnographer, might unwittingly take documents containing personal information out of the office or be exposed to information from the documents that I was not supposed to know (such as promotion or salary documents). He was apologetic but told me that I would lose access to the server as my knowledge of the files could jeopardize the team's work. By doing so, he was preventing a transitive risk to the other members of the team whose blame might be entailed by letting a putative outsider access their information in the first place.

While these two incidents appear to reflect the same kind of panic over potential documents leaks and inappropriate access discussed in the previous section, they also reflect an orientation to the roles employees took vis-_a-vis securitization. That is, during my main fieldwork in 2014–2015, employees, particularly managers, took on roles as active guardians of both documents and employees in their charge. In the first case above, the HR manager may have prevented viewing of such documents, but she also did not reveal the incident to others or report me to the auditing team. In the second case, the HR team's local server acted as a border within a border: such a private server was separate from the formal intranet service and was confined to the team's own workspace. It also served to define a team unit by both its shared knowledge and memory of work (the files), and by the knowledge and understanding of the existence of the server in the first place. The existence of such a server goes both beyond what an organization might require – securing and organizing documents on a shared local server, but also against what an organization might require in terms of common document security (as an "off-the-grid" server with no password). It also reflected the authority that teams at the time understood as the flexibility in document security measures. HR documents, for instance, are a particularly sensitive category within organizational documents and the team had other means of protecting such files (like filing cabinets with locks and special access restrictions on the group intranet). Nevertheless, potential breaches like mine could act as a means of socializing members to the unique professional challenges. (In another incident, the team manager took responsibility for an error that his junior team member made on a document that was given to the chairman). Managers had some autonomy to preserve their (team's) own documents [12]. Where employees might risk leaks, they might receive a scolding from their team manager, but not face other consequences of a more substantial leak.

It could be said that these cases reflected specificities of human resource practice (which tends to deal with individual employee information) or my own role as an outsider/ ethnographer. However, junior employees on different Sangdo teams exhibited concerns for documents in their own small spheres of practice in ways that went beyond simply legal or regulatory concerns, reflecting socialized norms for protecting documents. For instance, a few employees individually bought computer monitor filters to prevent passers-by from lunch or went home at night. Similarly, they used leatherbound folders when transporting documents from one department to another to conceal idle glances. These small acts reflect what Shires (2018) has termed "security rituals," or acts that enact images of security and secure behavior, but may not necessarily be related to specific security demands of an organization. Though junior employees were not as responsible or aware of the breadth of document security, they nevertheless exhibited their own forms of document protection in their own spheres of activity in particularly visible ways. When I returned to Sangdo in 2018 for a follow-up visit, Sangdo had undergone a significant change from when I had been there three years prior. An HR team manager informed me that the entire digital document

infrastructure of the Sangdo tower (which housed many of the companies in the group) had been "clouded." By "clouded," a term he coined in English, he referred to a new document storage and access system. Every single document at their office, the Sangdo holding company, was to be stored on company cloud servers, not local shared (team-based) hard-drives, nor even local computers. This would allow all documents to be encrypted, preventing their legibility by outsiders without an encryption key. However, this affected internal access as well: documents could no longer be simply copied or opened; they now had to now be requested, approved and accessed, reflecting a new layer of security-derived terminology for thinking about documents. Employees on the HR team reported that they now had to ask their team managers for approval to open even their own documents. This added layer of administration, in their comments to me, had rendered their organizational roles into one of document approvers and requesters, rather than HR specialists. Sensing the changes in the times, one team manager told me he was now learning the coding language R to add to his managerial toolkit. (As a company outsider at this point, I could only hear about how their changes were going rather than observe inside for any length of time).

An IT manager described the reasons for the new document storage system. It was developed at the request of company owners who were worried about document leaks and hacks, particularly about leaks of manufacturing secrets to overseas competitors. The IT manager explained this in the idiom of a criminal investigation: ownership had the power to trace a document if it ever got leaked, like CCTV. According to him, it was not necessary to actively prevent document leaks – documents could only be read with an encryption key as it were, rendering other forms of security somewhat moot. But attention toward individual responsibility around documents was heightened: new metadata scripts allowed IT managers to go back to a log of activity and see which employees last had access to a particular document and then narrow down potential suspects for fraud or malpractice, making it easier to identify or prosecute leakers, ill-intentioned or not.

This development reflects a more general trend linking the digitalization of work with the securitization around leaks that has affected many office-based and document-dependent workplaces in recent years. (It is fair to say even academics have become literate in concepts like multi-factor authentication these days.) Yet the ethnographic observations from Sangdo reflect a subtle shift in the implicit roles that managers and employees had in the system of protection. In the pre-"clouded" environment, managers had the authority to preserve and store their own documents in their own ways, and monitor the conduct of their own employees. This reflected an ethos that was managerial in nature: while following some general rules, managers were responsible for the conduct of their team's documents and were delegated the authority to do so. In the cloud-based encrypted system, all documents had become objects of a crime-based approach to security which in turn flattened employees to "users" with specific kinds of access rights; mistakes, in theory, had a quasi-criminal, not just a moral, quality to them. Where once managers had a remit of authority around their own members, the IT function was now taking on new powers of control over work practice and the securitization of both people and documents across many teams. While the examples from seeing their screens. They also covered drafts of documents with blank paper, flipped them over or filed them in drawers to prevent inadvertent viewings when they left their desks for Sangdo represent one development in this direction, a recent report from Nikkei Asia about South Korean technology giant Samsung suggests that the future direction of security

technologies centered around document tracing may intertwine technological sophistication and individual criminalization in even more complex ways:

> At one [Samsung] laboratory, the printing paper used in copying machines contains metal foil, part of a detection system intended to stop employees from printing out sensitive information and taking it out of the lab without permission. Alarms sound if the paper leaves the building [13].

Conclusion: emerging ethnographic barriers

This article has discussed the increasing securitization of document leaks in contemporary organizational ecosystems. By securitization, I have adapted a term from international relations and focused on the ways that documents are increasingly treated as protected objects within organizations, a fact evident in the rarity of organizational files being shared in public as well as the increasing number of security apparati dedicated to storing, securing and more often, encrypting digital files in ways largely indiscriminate of genre or content. A key part of this securitization is the linking of employees to document circulation, through new technologies and policies that can individuate their relationship to documents [14]. Despite millennial narratives that predicted or advocated a gradual paperless worklife, documents and the arts of documentation are deeply woven into contemporary corporate work worlds, in South Korea as elsewhere (Sellen and Harper, 2003). This is certainly true in terms of coordinating work among distributed teams; but I have also suggested that it is true in terms of thinking about documents as fictive property in an information age, whether or not files are actually valuable in circulation. Files might contain intellectual property, personal information or company secrets, but in many cases they are coming under a blanket bureaucratic logic of protection. Here returning toWeber is useful: where he might have predicted that bureaucratic domination results in the "leveling of "status honor"' (Weber, 1978, p. 975) among people – such as in this case, going from guardians of company documents to simply users equal under IT – the same can also be said of leveling among document genres. Under an IT lens, documents lose many of their substantive qualities as types with meaning and context and are largely treated the "same" when rendered as "data" or "files" that must be preserved by virtue of where they were produced.

Such securitization is not necessarily leading to the kind of organizational secrecy as transparency advocates might predict or fear. Such concerns imply that employees or insiders are motivated to gird themselves against outsiders; rather, the dynamic here is one in which the "inside" is being gradually separated from the human actors that occupy it, leaving an inventory of documents qua property. This explains the close integration of digitalization with techniques of individuation. The ethnographic data from the South Korean organization Sangdo emphasized how this security turn represents an increasing focus on individuals as the bearers of responsibility. Through encountering a shift in how documents were preserved at Sangdo, I noted that the role of managers and employees was also shifting in relation. This led to a case in which even high-level managers were being associated suspiciously in regards to such objects of security, rather than as their guardians. Such concerns are never completely unfounded of course; leaks do happen and can cause material harm to individuals or organizations. However, securitization logic can spread categorically, rendering substantive differences or local workarounds problematic. In this regard, South Korea's increasingly digitized and high-speed workplaces reflect not just a place to consider one possible future of

an evolving digital workplace, but an environment marked by increasing securitization which is shifting the relationship between employee and organization.

Increasing securitization of document leaks will have an impact on ethnographic research across many types of organizations in three ways. First, securitization may delimit access to domains of organizational practice for ethnographers to see, discuss or even collect certain artifacts accessing a field. Document protection itself is a new kind of gatekeeper, in other words. Ethnographers may not face difficulty in interviewing, following, or being in an organization, but may be relegated to areas of an organization that befit someone with "lowlevel" access. Discussions with higher-level or more sensitive work areas may be limited to interview interfaces, away from sites of actual practice. There is of course much to be gained from techniques of "polymorphous engagement" by interacting with organizational actors outside of organizations (Gusterson, 1997) and collecting publicly available documents (Zilber, 2014, pp. 102–104), especially to remove the prestige and "mysterium" (Grey and Costas, 2016) that is often accorded to insider spaces. But it is worth pointing out how document secrecy concerns may be one reason for organizational (in)accessibility in the first place. Document security and its "rigid designators" for user-based access control might be shaping the terms and limits of an ethnographer's access to a field. At Sangdo, I benefited from researching the company at a time in 2015 when managers had more autonomy over document storage and I had some freedom to peruse what I could. To conduct research in 2018 when they implemented the "cloud" system would have vastly changed what I could have perused, asked about, or collaborated on. Second, an ethnographer's relationship to employees or other organizational actors will be altered as new risk vectors emerge in relation to documents in the field. As I have alluded to in this article, South Korean employees are highly attuned to who has access and how this might implicate themselves or others. Moreover, increasing use of metadata and paper-based tracking to trace the origins and movement of files may create new paper-trails for employees in sharing files with ethnographers, even when satisfying other institutional research demands. Ethnographers themselves may face unknown risks depending not only on what questions they ask, but what files they see. Third, there may be increasing legal and IT conditions to what ethnographers can analyze out of the field. Even if document data is properly anonymized and circulated for purely academic purposes, it may fall under logics of increasing digital criminality and malfeasance that go beyond traditional university-based ethical reviews. Like the IT manager who described the CCTV-like ability to trace back documents, considerations of documentary traceability may be a concern even if they do not pose a perceivable risk at the level of informant or subject relations.

Critical approaches to securitization are meant to ultimately question the basis of why security "problems" exist and at what political ends they are aimed. My adaptation of the concept here – to understand securitization in an organizational setting – suggests that it will not be so simple just to unmask the many layers of legal, regulatory, digital and normative security toward documents that intersect contemporary organizations. As part of the ethnographic process, ethnographers may need to become literate in the basics of organizational (cyber) security as well as spell out terms of access at the beginning of projects, especially as informal workarounds become excised. Furthermore, they may also need to creatively figure out ways of accessing sites of practice without compromising research participants or informants, such as by asking for "blank" document templates, collecting old printouts or working on files in situ without "moving" them and leaving a

digital trace. Ethnographers might even topicalize everyday security as part of the research project to understand how employees live with and make do in new security environments where they are being recast from privileged insiders to insider threats. This may also involve new subjects of organizational research. Much of my knowledge of the IT infrastructures and systems at Sangdo and in the South Korean corporate world came unexpectedly from coworkers in IT roles who were friendly enough to describe security changes and effects without disclosing actual files. In this sense, the myriad barriers ethnographers face in a securitized workplace are not just something to get past, but themselves should become part and parcel of ethnographic investigation itself.

One future direction for the study of insider-ness vis-_a-vis securitization is to reconsider not only the ethnographer-subject or ethnographer-organization role, but how internal boundaries are also being reshaped along these lines as well. This is already apparent with auditing or oversight institutions which can claim access to documents (through audits) or create their own document standards (such as financial reporting). Quarterly financial reporting, and the bevy of financial templates that accompany it, is one way in which a relationship of external governance is premised precisely on a kind of legitimized document exfiltration that has become normalized over time. Here, the "security" question elides with governance issues, as large corporations, particularly publicly traded ones, must submit themselves to certain kinds of "leaks" of their information lest they be deemed financially opaque. However, another relationship merits attention: organization-internal relations of documentary security. Leaks are clear boundary-crossing events as they go from a private to a public space, but we might ask about when a document moves from one office to another. Commonsense as it is to treat organizations as bounded units, organizations like Sangdo are complex conglomerates that have clearly delineated subsidiaries and offices. How might employees be judged if they share documents with another team or an IT department grants access to confidential files to all executives but not upper-level managers? How might a headquarters establish relationships with its subsidiaries through document requests, or conversely, institute new disciplinary measures for document misappropriations? Difficulty of access aside, issues that involve the ambiguity of internal borders, the bureaucratization of organizational life and the complexity of material practices are ripe for new kinds of ethnographic encounters. While the new securitized workplace is not going away, it may afford new questions even as it redefines barriers for insiders and outsiders alike.

Notes

1. Indeed "new" organizational forms premised on models of sharing, transparency or open networks go against this account, but I would suggest that their organizational novelty highlights that a larger majority of organizations are bound by increasing strictures of document and information security, especially in an era of international data protection regulations and cyberattacks.
2. See for instance the Software Engineering Institute of Carnegie Mellon University which has become a leading hub of expertise on cyber security and insider threats. Such research hubs naturalize a sense of criminality that surrounds employees when it comes to digital work: "[E]mployees can become easy and willing targets of pressure from criminals and foreign agents, or they might become disgruntled and careless on the job." Source: https://www.sei.cmu.edu/our-work/ insider-threat/index.cfm. Accessed September 9, 2019.

3. Each co-worker on the HR team formally consented to be part of a long-term study on office social life and other employees who I interviewed consented to the research protocol as well.
4. Sangdo is an example of what is known in South Korea as a daegieop ("large corporation") or geurubsa ("group company"). Organizationally, the Sangdo Group had around a dozen subsidiaries involved in metal and steel manufacturing. The subsidiaries were linked, as in many other Korean conglomerates, by a holding company which also had certain centralized managerial powers. An owning family had a majority control over the holding company.
5. For Gitelman, the protagonist of modern digital document infrastructures is not the database, the hypertext or HTML, but the PDF (Gitelman, 2019). As an exemplar format, the PDF coheres information into a form of fixed pseudo-property to prevent it from being edited, re-authored or recombined. A PDF, or portable document format, is the documentary equivalent of a universal Turing machine. Based on PostScript language, a PDF file can reproduce documents from other programs into an image, rendering them into a common, intermodal format, around which other machines, codes and services revolve (Dourish, 2017, pp. 18–22).
6. Such dynamics parallel debates around "data sovereignty" which envisions data control as a matter of territorial control. See Amoore (2018).
7. This is not to say there are no studies of documents or other written genres. However, many studies of office documents talk about documents, but are rarely able to re-present them or their contents.
8. Former President Park also had a blacklist of almost 10,000 public figures and artists who were critical of her and who would not be granted state funding as a result.
9. South Korea instituted a comprehensive data protection act called the Personal Information Privacy Act (PIPA) in 2011 which strictly regulated the storage and circulation of personally identifying information (PII) by organizations that manage it. It has a close resemblance to the European Union's General Data Protection Regulation (GDPR) which was instituted in 2018. Agencies such as the Ministry of Interior and Safety regularly levy fines for companies that improperly manage personal data or allow documents containing personal information to leak, even during a cyberattack.
10. The method of cutting off certain parts of a document to make it "circulable" is not unlike what Daniel Ellsberg did when copying the files that would later become bundled together as "the' Pentagon Papers. With his helpers, he cut off the tops and bottoms of documents on which were written "TOP SECRET," so as not alert those at photocopy shops (Gitelman, 2014, p. 89).
11. I have noted elsewhere (Prentice, 2015) how the semi-illicit circulation of documents (through former colleagues or previous projects) can prove to be useful in consultant work in South Korea.
12. The fact that a separate "private" border was constructed reflects the way that categories of private and public or inner and outer have a "recursive" quality to them, as discussed by anthropologist Gal (2002). Ahome, for instance, is private relative to the public outside, but a bedroom might be private relative to a living room. The concepts are about the deployment of a boundary-bearing distinction, not about absolute boundaries in and of themselves. Any workplace exhibits this feature, as there are waves of both public areas and private areas, which can then be divided into further public and private distinctions (such as the lobby in front of an executive's office.)

13. “Samsung races to guard its secrets as China rivals close in” Nikkei Asia. February 12, 2021. https:// asia.nikkei.com/Business/Business-Spotlight/Samsung-races-to-guard-its-secrets-as-China-rivalsclose- in
14. Hull (2003, pp. 287–8) has described how one of the basic features of bureaucratic techniques is its role in individuating action so as to affix responsibility for decisions.

REFERENCES

Amoore, Louise. 2018. "Cloud geographies: Computing, data, sovereignty." Progress in Human Geography 42 (1):4-24.

Bittner, Egon. 1965. "The Concept of Organization." Social Research 32 (3):239-255.

Buzan, Barry, Ole Wæver, and Jaap De Wilde. 1998. Security: A new framework for analysis. Boulder, Colorado; London: Lynne Rienner Publishers.

Czarniawska, Barbara. 2008. A theory of organizing: Edward Elgar Publishing.

Dahles, Heidi, and Loh Wei Leng. 2005. "Boundaries and organizations in Asia: an introduction." Asia Pacific Business Review 11 (4):449-460.

Diesner, Jana, Terrill L Frantz, and Kathleen M Carley. 2005. "Communication networks from the Enron email corpus "It's always about the people. Enron is no different"." Computational & Mathematical Organization Theory 11 (3):201-228.

Dourish, Paul. 2017. The stuff of bits: An essay on the materialities of information: MIT Press.

Dourish, Paul, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. "Security in the wild: user strategies for managing security as an everyday, practical problem." Personal and Ubiquitous Computing 8 (6):391-401.

Fenster, Mark. 2005. "The opacity of transparency." Iowa L. Rev. 91:885.

Fenster, Mark. 2015. "Transparency in search of a theory." European journal of social theory 18 (2):150-167.

Gal, Susan. 2002. "A semiotics of the public/private distinction." differences 13 (1):77-95.

Garfinkel, Harold. 1967. Studies in ethnomethodology. Englewood Cliffs, N.J.: Prentice-Hall.

Garsten, Christina. 2010. "Ethnography at the Interface: "Corporate social responsibility" as an anthropological field of enquiry." In Ethnographic practice in the present, edited by Marit Melhuus, Jon P. Mitchell and Helena Wulff, 56-68. Oxford: Berghahn Books.

Gitelman, Lisa. 2014. Paper knowledge: Toward a media history of documents. Durham, NC: Duke University Press.

Gitelman, Lisa. 2018. "Publication Date: September 11, 1998." Full Stop Reviews, 8-15.

Grey, Christopher, and Jana Costas. 2016. Secrecy at work: The hidden architecture of organizational life: Stanford University Press.

Gusterson, Hugh. 1996. Nuclear rites: A weapons laboratory at the end of the Cold War: Univ of California Press.

Gusterson, Hugh. 1997. "Studying up revisited." PoLAR: Political and Legal Anthropology Review 20 (1):114-119.

Hull, Matthew. 2003. "The file: agency, authority, and autography in an Islamabad bureaucracy." Language and Communication 23 (3):287-314.

Jin, Dal Yong. 2017. Smartland Korea: Mobile Communication, Culture, and Society. Ann Arbor, MI: University of Michigan Press.

Kirsch, Thomas G. 2019. "Securing Security." In Spaces of Security: Ethnographies of Securityscapes, Surveillance, and Control, edited by Setha Low and Mark Maguire, 122-140. New York: New York University Press.

Maguire, Mark, and Setha Low. 2019. Spaces of security: ethnographies of securityscapes, surveillance, and control. New York: NYU Press.

McDonald, Matt. 2008. "Securitization and the Construction of Security." European journal of international relations 14 (4):563-587.

Monahan, Torin, and Jill A Fisher. 2015. "Strategies for obtaining access to secretive or guarded organizations." Journal of Contemporary Ethnography 44 (6):709-736.
Ortner, Sherry B. 2010. "Access: Reflections on studying up in Hollywood." Ethnography 11 (2):211-233.
Park, Dongoh. 2015. "Social Life of PKI: Sociotechnical Development of Korean Public-Key Infrastructure." IEEE Annals of the History of Computing 37 (2):59-71.
Paulsen, Neil, and Tor Hernes. 2003. Managing boundaries in organizations: Springer.
Prentice, Michael M. 2015. "Managing Intertextuality: Display and Discipline across Documents at a Korean Firm." Signs and Society 3 (S1):S70-S94.
Rumford, Chris. 2013. Citizens and borderwork in contemporary Europe: Routledge.
Schüll, Natasha Dow. 2018. "Digital containment and its discontents." History and Anthropology 29 (1):42-48.
Scott, W Richard, and Gerald F Davis. 2015. Organizations and organizing: Rational, natural and open systems perspectives: Routledge.
Seaver, Nick. 2017. "Algorithms as culture: Some tactics for the ethnography of algorithmic systems." Big Data & Society 4 (2).
Sellen, Abigail J., and Richard H.R. Harper. 2003. The Myth of the Paperless Office: MIT Press.
Shires, James. 2018. "Enacting expertise: Ritual and risk in cybersecurity." Politics and Governance 6 (2):31-40.
Souleles, Daniel. 2018. "How to Study People Who Do Not Want to be Studied: Practical Reflections on Studying Up." PoLAR: Political and Legal Anthropology Review 41 (S1):51-68.
Turco, Catherine J. 2016. The Conversational Firm: Rethinking bureaucracy in the age of social media. New York, NY: Columbia University Press.
Weber, Max. 1978. Economy and society: an outline of interpretive sociology. 2 vols. Berkeley: University of California Press.
Weber, Max. 2004. "Politics as a Vocation." In The Vocation Lectures, edited by David Owen and Tracy B. Strong, 32-94. Indianapolis: Hackett Publishing Company.
Yang, Sunyoung. 2017. "Networking South Korea: Internet, nation, and new subjects." Media, Culture & Society 39 (5):740-749.
Yates, JoAnne. 1982. "From press book and pigeonhole to vertical filing: Revolution in storage and access systems for correspondence." Journal of Business Communication 19 (3):5-26.
Yates, JoAnne. 1989. Control through communication: the rise of system in American management, Studies in industry and society. Baltimore: Johns Hopkins University Press.
Yost, Jeffrey R. 2015. "The Origin and early history of the Computer Security Software products industry." IEEE Annals of the History of Computing 37 (2):46-58.
Zilber, Tammar B. 2014. "Beyond a single organization: Challenges and opportunities in doing field level ethnography." Journal of Organizational Ethnography.