Technological change and users: An actor-network perspective on the digitalization of video surveillance

Weaver, Benjamin; Lahtinen, Markus

2011

Technological change and users:

An actor-network perspective on the digitalization of video surveillance

Benjamin Weaver
Institute of Economic Research
School of Economics and Management
P.O. Box 7080
SE-220 07 Lund
benjamin.weaver@fek.lu.se

&

Markus Lahtinen
Institute of Economic Research
School of Economics and Management
P.O. Box 7080
SE-220 07 Lund
markus.lahtinen@ics.lu.se

LUND
UNIVERSITY

Technological change and users:

An actor-network perspective on the digitalization of video surveillance

Abstract

This paper discusses aspects of technological change and the path towards institutionalization of new innovations, with a focus on how users matter and are part of the co-construction of such change. An empirical example from the security industry is used to illustrate how two distinct phases in the analog-to-digital shift in video surveillance technology have had very different outcomes with respect to the pace and nature of user adoption. The notions of actor-networks and communities of practice are used to analyze the different user and industry reactions to the introduction of the digital video recorder (DVR) and the network video camera respectively. The analysis focus on how established industry socio-technical actor-networks encompassing users incumbent industry and technological artifacts can resist attempts of disruptive innovation technological change from powerful outside forces.

Key words: technological change, security industry, video surveillance, actor-network, communities of practice

Introduction – users and technological change

That users play a key role in relation to technological innovation and technological change is rather self-evident. No matter how useful or groundbreaking, a technology that is not accepted and adopted by users is likely to be discarded to the scrap heaps of innovation history, where artifacts such as the plastic bicycle (Hult, 1992) and the electric plough (Todd, 1992) lay buried. But users also play a key role in shaping technology, as in the case with the success of the Short Messaging Service (SMS), which was originally intended solely as a unidirectional messaging service whereby customers could receive service messages such as voice mail notifications (Taylor & Vincent, 2005). However, as early users (particularly young pre-paid subscribers) discovered an infrastructural loophole that enabled them to send free text messages to each other, SMS was quickly popularized and operators soon adapted its business models to include SMS as an integral part of mobile services (Taylor & Vincent, 2005).

Yet, in the area of innovation and technology studies within management and sociology the user perspective is arguably overlooked and under-theorized. In mainstream economic and management literature technology is typically treated from a supply-side perspective. In neo-classical economic theory, technological change in the form of innovations that improves the "instructions for mixing together raw materials" (Romer, 1990, p. 72) is the key driver of economic growth. The nature of such technological change is not explored in neo-classical analysis, and technology is thus seen as something that develops according to an inherent logic. This internalist (Hughes, 1986; Nye, 2006) or deterministic (Williams and Edge, 1996) view on technology tends to focus the attention on how society and people adopt to the effects of technological change, rather than how this change is actually shaped by society and people (MacKenzie and Wajcman, 1999, p. 5).

As in economics, and given the focus on issues such as value creation, competitive advantage, and organizational efficiency, analysis of technology in mainstream management and organization studies literature also tends to put the focus on the supply side. Technology in and of itself is rarely a variable under analysis, reflecting a determinism that often takes the form of implicit assumptions, or technological change being taken for granted (Pinch and Bijker, 1984). However, notwithstanding that the underlying perspective of technology

development, the effects of new technology on industries and organizations and the capabilities that enable firms to innovate, and commercialize new technology are central themes in management research. Specifically, firms and industries have often been found to be path dependent (Arthur, 1989, 1990), which may block the organizational adoption of new technologies (Henderson & Clark, 1990; Leonard-Barton, 1992).

In the Schumpeterian-influenced strands of research that focuses specifically on technological change and (disruptive) innovation, the focus is often the entrepreneurial activities involved in innovation work. Literature in this vein tend to take step away from determinism, by acknowledging the cyclicality, complexity and historical path dependence of technological innovation. As one of the forerunners in this field, Dosi (1982) imported Kuhn's (1967) paradigm metaphor to describe the emergence of new technology, thereby opening up for a stronger focus on the social shaping of technological change, partly through a Schumpeterian emphasis on innovators (firms or entrepreneurs) and the innovative process, but also through the notion that a paradigm establishes itself as a shared "outlook" or specific perspective on technology (Dosi, 1982, p. 152) among e.g. engineers in a company or an industry, that essentially blocks outs competing paradigms. The most influential research in this area, however, is often attributed to Christensen (1997) and his studies of the failure of incumbents to respond to the emergence of disruptive innovations. While Christensen's work is based on solid business history work and an analysis that can hardly be considered deterministic, it has been criticized for (among other things) its shallow analysis of the demand-side role in disruptive innovation (Adner, 2002).

In more historically and sociologically oriented research on technology, which typically rejects determinism and embraces the social embeddedness (Granovetter, 1985) and contextuality (Nye, 2006) of technology, Yates (2006) finds that a similar lack of user-oriented focus has traditionally been the norm, although a 'demand-side turn' has emerged in recent decades. According to Yates (2006), however, this demand-side turn has typically focused on either individual users of technology, or on government and state organizations, e.g. the military and the public sector. This is particularly reflected in the research carried out within the program of social construction of technology (SCOT) that emerged in the early 80s. SCOT (Pinch and Bijker, 1984) set out to trace the historical origins of technology by

studying how technological artifacts are socially shaped by their relation to 'relevant social groups', where users always play an important role (e.g. Oudshoorn and Pinch, 2003). However, in line with the research interests of SCOT scholars and the program's roots in science and technology studies (STS), empirical work has rarely focused on commercial firms as users, leaving this particular niche under-researched from both management and sociological perspectives.

This paper will discuss aspects of technological change and the institutionalization of technology, with a focus on how users matter and are part of the co-construction of such change. After reviewing some common theoretical perspectives, a case study is presented, highlighting an empirical instance of technological change in the security industry, where it is argued that users have played a crucial role in shaping the pace of the migration from analog to digital platforms. The empirical material is then discussed in relation to the theoretical discussion, and finally some conclusions are made regarding the implications of the findings.

Technology as institution and socio-technical network

As rival technologies vie for dominance in a market, a number of factors will contribute to the eventual emergence of a technological standard or 'dominant design' (Anderson and Tushman, 1990). As studies of history of technology have shown, it is far from always that the 'best' technology or superior standard emerges dominant in the end. Rather, as argued by Arthur (1989 p. 116) it may be the technology that, by random chance, first achieves traction with users that eventually emerges successfully:

> Modern, complex technologies often display increasing returns to adoption in that the more they are adopted, the more experience is gained with them, and the more they are improved. When two or more increasing-return technologies 'compete' then, for a 'market' of potential adopters, insignificant events may by chance give one of them an initial advantage in adoptions.

Hence, a coincidental chain of events may set off a technology on a successful trajectory that eventually block out competing alternatives. The advent of the QWERTY keyboard represents

the classic case (Arthur, 1989; Greener, 2002), where an inferior technology – due to a series of stochastic events – came to dominate the design of keyboards for an indefinite amount of time. The QWERTY keyboard can thus be said to have become an institution, as described by Pinch (2008, p. 467):

> The embedding or freezing of choices within scientific and technical systems […] makes technology actually one of the most powerful institutions […] we as social scientists face. It is because social choices appear to have vanished from technologies, or are so deeply embedded within technical structures that they become invisible to all but the technical experts, that technologies are powerful institutions.

However, few technologies or standards exhibit as strong path dependencies and lock-in effects as the QWERTY keyboard. Under certain circumstances and in certain contexts it becomes possible to deviate from the path or even create completely new paths (Greener, 2002) – such as in the cycles of radical disruption. As shown by e.g. Pinch (2008), on the development of the Moog synthesizer, users of technology, both shape and reinforce such technological institutions. A key aspect of the success of the Moog was that Moog (the inventor) was more responsive than his competitors to the needs and opinions of the musicians that would make up his customer base. Moog thus explicitly allowed users to co-construct what became the technological standard or "path dependence" for the early synthesizer (Pinch, 2008).

A key component in most theories of technology is thus the notion of a newly developed technology reaching a stage where it develops into a standard that is path-dependent, and can even be considered an institution. This end-point of technological innovation and change has been given many names, including technology paradigm (Dosi, 1982) and dominant design (Anderson and Tushman, 1990). In SCOT, the final analytical step deals in the analysis of closure and stabilization of technological artifacts (Pinch and Bijker, 1984). Pinch and Bijker (1984) define two types of closure: Rhetorical closure – where the problem is solved by shaping the meaning that different social groups attach to an artifact, e.g. through advertising. Closure by redefinition of the problem, can be achieved by proving the superiority (or additional benefits) of the artifact along some new performance dimension that might not have been apparent in previous iterations of the artifact.

One perspective that has proven particularly useful for describing and analyzing the links between science, technology and the 'social' is actor-network theory, or ANT. In ANT, the technology and the social world are intrinsically seen as linked in heterogeneous networks, in such a way that "society, organizations, agents, and machines are all effects generated in patterned networks of diverse (not simply human) materials" (Law, 1992 p. 380). Everything in society is thus connected to such socio-technical networks, comprising both artifacts and humans – or *actants* – in complex ways (Latour, 1991). ANT is less a theory of the social, and more a method to trace and describe how *associations* between heterogenous actants are made and transformed (Latour, 2005). By employing such a 'flattened ontology', dichotomies such as society/technology, actor/object and local/global are rejected (Latour, 2005) in favor of a symmetrical treating of humans and non-humans (Latour, 1987; 2005).

Technology, or materiality, is thus not separate from the social but rather is described by Latour (1991, p.129) as "the moment when social assemblages gain stability by aligning actors and observers". Technological artifacts become actants that can be described as "programs of action coordinating a network of roles" (Callon, 1991, p. 136). When specific network constellation – e.g. a railway system or a television – work as a "single block" and perform a function, they tend to become concealed and disappear, being only perceived through the action they perform (Law, 1992). This *simplification* (Law, 1992) or *stabilization* of networks (Latour, 1991) is desirable and constitute the underpinning of society, or in the words of Latour (1991, p. 129): "when actors and points of view are aligned, then we enter a stable definition of society that looks like domination".

Latour (1987, 1991) also uses the metaphor of the "black box", originally as way to describe how scientific controversies are settled. The "black-boxing of longer and longer chains of associations" (Latour, 1991) leads to stabilized networks that can be more or less durable. Networks may start out as a thought – which is fleeting and unstable – but when the original thought eventually becomes embodied in material form such as text and technological artifacts, a durable network may emerge over time (Law, 1992). But materiality is not a guarantee of durability per se, as any material artifact may become part of other networks and their purpose or use might change completely (Law, 1992). An army base may converted into a business park in times of peace, say, or a computer may come to perform the function of a

telephone or a television by way of being connected to the Internet. Such transformations occur and are enabled through processes of *translation* (Callon, 1986; Latour, 1991; Law 1992) whereby the roles and relationships between actants and networks are continually deconstructed, reconstructed and reconfigured.

Actor-network theory is especially applicable when socio-technical controversies arise (Latour, 2005), e.g. in times of innovation and disruption, when black boxes that have become taken for granted are reopened (Latour, 1987). During such controversies, associations are rendered particularly visible, as the processes of transformation and translation leads to the break-up and re-creation of actor-network constellations and black boxes. From a methodological point of view, actor networks can be traced by identifying a point of departure, e.g. an actor that wishes to establish a new technological product on the market, which is identified as a program of action (Latour, 1991) to which other actors may respond to by launching anti-programs, as a way of resistance.

Actor-network theory can also be helpful in highlighting the role of technology users or end-customers. Latour (1987) is critical to traditional technology diffusion models, that puts too much focus on innovators and their great innovations in explanations of technological development while ignoring or downplaying the role and impact of other social actors, such as users:

> Diffusionists simply add *passive* social groups to the picture that may, because of their own inertia, slow down the path of the idea or absorb the impact of the technics. In other words, the diffusion model now invents *a society* to account for the uneven diffusion of ideas and machines. In this model society is simply a medium of different resistances *through which* ideas and machines travel. […] This has been called the principle of *asymmetry:* there is appeal to social factors only when the true path of reason has been 'distorted' but not when it goes straight. (Latour, 1987 p. 136).

Latour (1987) is also critical of the notion that once a black box – e.g. a new technologically advanced product – is ready to be deployed on a market, end-users are reduced to 'simple customers' that either buy the product (or don't). For Latour (1987) there are no such 'simple customers'. Rather, the "more automatic and blacker the box, the more it has to be accompanied by people" (Latour, 1987 p. 137). Latour (1987) points to the successful

introduction of Eastman's Kodak film camera in 1888. Launched with the seminal slogan "you press the button, we do the rest", the Kodak camera was highly automated and easier to use compared to the complex plate cameras that preceded it. Yet, while Kodak's camera was indeed a highly successful example of a 'black box', its actual functioning depended on the development of a vast commercial network that encompassed film and camera manufacturing, distribution and developing services. The Kodak camera system thus required the recruitment and interaction of a large number of people as well as active customers, that all had to associate themselves with the 'black box', which Latour (1987, p. 139) defines as being successful when it "concentrates in itself the largest number of hardest associations".

In summary: through the rejection of technological determinism comes the realization that, throughout society, technology and people are intertwined in socio-technical networks. A great deal of intellectual effort has been devoted to the understanding of how such socio-technical networks evolve into what can be called institutions, and how technology and the social world co-construct each other. As shown in the above, socio-technical institutions have been given many labels: technological 'paradigm' or 'standard', 'dominant design', 'path dependence' a 'black box' or a stabilized 'actor-network' containing chains of particularly strong associations. Regardless of the perspective chosen, a central theme is the continuous cycle of innovation-dominance-disruption, whereby even the most stable socio-technical institution eventually crumble and give way for something new. Traditional perspectives, within e.g. economics and management, tend to focus on the innovative process itself, while largely ignoring the finer and 'messy' social and technical details of how a particular technology is adopted or not and shaped by users and other relevant groups. This has left the field wide open for sociologically oriented research programs such as SCOT and ANT. The latter has been particularly successful in highlighting the complex linkages between people and technology, by allowing for an equal analytical treatment of technology as well as people.

Technology users, skills and communities of practice

As shown above, technology, is both shaped by and a shaper of society and can be seen as an institution that is embedded in socio-technical networks between human and material objects. In such a scheme, users of technology are naturally important stakeholders. Professional users working within specific domains need to hold certain skills that are often intrinsically connected to technology and artifacts such as machines, or as argued by Callon (1991, p. 138): "No description of skill is possible unless the networks and humans, text and machines within which they are expressed and put to work are constituted". Humans, skills, and machines are thus interconnected in layers of networks that transcend formal organizational structures.

The analysis of such networks of professionals have received considerable interest within streams of research such as that devoted to "communities of practice" (Brown and Duguid, 1991; Wenger, 2000) or the literature on professions and professionalization (Eriksson-Zetterquist et. al, 2009). The communities of practice perspective entails studying learning and work in a practice in the actual settings and contexts where they happen, rather than focusing on e.g. the intentions, plans or descriptions given by managers (Brown and Duguid, 1991). What often emerges is the divergence between canonical vs. non-canonical practice, i.e. the difference between how work and tasks are prescribed and the way they are carried out among groups of practitioners (Brown and Duguid, 1991). Non-canonical communities of practice also tend to transcend formal organizational boundaries, and extend to e.g. suppliers and customers in a value chain. For Fox (2000), this links the communities of practice perspective with ANT, in that both perspectives question the formal organization as the most relevant unit of analysis:

> COPs [communities of practice] which spans buyers and suppliers, sellers and customers, acquisition teams and competitors are just some of the promiscuous interstitial communities where translation, enrollment and and mobilization are going on: shaping the boundary of the formal organization incidentally or as an after-thought (Fox, 2000, p. 865).

The actor-network perspective, with its focus on associations between actors in heterogeneous network formations, thus lends itself well for an analysis of how communities of practice evolve, learn and transform across formal organizational boundaries.

A number of researchers have also explicitly explored how the introduction and implementation of new technology affects the social relations within communities of practice or groups of practitioners in organizations (Eriksson-Zetterquist et al., 2009; Barley, 1986, 1990; Edmondson et al., 2001). According to Eriksson-Zetterquist et al. (2009, p. 1148), citing Barley (1990), it is important in such instances to focus on "the status of various skills and competencies in the actual social setting". Hence, to assess technology's impact on social relations it is important to study it at the level and location where it is implemented and used.

Tushman and Anderson (1986) link the local, organizational effects of new technology on skills, to larger technological shifts at the macro-level, e.g. shifts within or across entire industries. They distinguish between competence-destroying or competence-enhancing technological shifts according to the effects they have at the industry level. Competence-destroying discontinuities "are so fundamentally different from previously dominant technologies that the skills and knowledge base required to operate the core technology shift" (Tushman and Anderson, 1986 p. 442). The effects of such shifts can thus be radical at the organizational and individual level, as firms and employees may find that their skills are rendered obsolete. In contrast, competence-enhancing changes in technology are gradual improvements in performance or price that follow previous technology path trajectories and thus do not require new skills (Tushman and Anderson, 1986).

However, even when a technological shift may appear logical and rational at a macro level, the process of change at the local and social level, may be a lot "messier", political and dynamic, as described by Barley (1990, p. 67):

> Technologies are depicted as implanting or removing skills much as a surgeon would insert a pacemaker or remove a gall bladder. Rarely, however, is the process of technical change so tidy. Events subsequent to the introduction of a technology may show that reputedly obsolete skills retain their importance, that new skills surface to replace those that were made redundant, or that

> matters of skill remain unresolved. In any case, groups will surely jockey for the right to define their roles to their own advantage.

Barley (1990) thus suggests that the social effects of technological change have to be studied in and from the perspective of the local social setting where practice takes place. Barley (1986) found that a shift to computed tomography technology occasioned very different structural outcomes in two separate radiology departments, suggesting that structuring is contextual and dependent on local social patterns and path dependencies. Edmondson et al. (2001) reported similar findings from a study of how routines changed following the introduction of a new surgery technology in 16 hospitals. The authors showed that the variance in local contexts at a group (rather than organizational) level of analysis played an important role in shaping group learning and the organization of work during the implementation of the new technology. In an investigation of purchasing professionals in the automotive industry facing new technology in the form of an EDI-based purchasing system, Eriksson-Zetterquist et al., (2009 p. 1164) showed how "technology, politics, ideology, and managerial practices jointly shape and influence professional communities". Noting that the purchasers were less integrated and organized as a professional group than compared to e.g. medical practitioners, Eriksson-Zetterquist et al. (2009), found that the introduction of new technology had a competence-destroying effects on purchasers, whose roles and social relations were changed and, resulting in lower organizational status for the group as a whole.

To summarize, most specialized professions today involve the use of technology in one way or another. Drastic instances of technological change may have competence-destroying effects on entire professions within and across industries and organizations. Learning and legitimization of new technology often occurs within communities of practice encompassing networks that span formal organizational boundaries. To understand technological change from the perspective of a practitioner thus involves developing an understanding of both the community of practice that the professional is part of as well as the local context where a new technology is implemented.

Methodological exposition

The paper is based on empirical data collected by the Lusax research group[1] in the period 2006 – 2011. The Lusax project is a collaboration – broadly guided by 'Mode 2' principles (Nowotny et al., 2003) – between the security industry and the Institute of Economic Research, Lund University.

Data for this paper has been collected cumulatively over the entire course of the research project. The geographical focus has been on Western Europe and the US, with an emphasis on the US and Sweden. Although mainly based on a qualitative case study / ethnographical approach, quantitative methods such as surveys have also been employed. Between the two researchers, 300+ personal interviews with all types of industry participants have been carried out, with an estimated average length of 1,5 h. Typically, following a grounded theory approach, these interviews have taken the form of unstructured or semi-structured interviews, guided by a rough set of guiding questions prepared for each interview. Interviews have been recorded whenever possible and transcribed to provide documentation for analysis.

In addition to interviews, significant time has been devoted to participant observation of e.g. industry and end-user meetings and conferences, participation at industry trade shows, as well as job shadowing of industry professionals. Between the two researchers, about 2-3 months of full-time research have been devoted to such ethnographic fieldwork activities. A number of secondary sources, documents (e.g. annual reports), trade press, market data and market reports, statistical reports, industry-related literature etc. have also been used at all stages of the research project.

The rich empirical material collected has been analyzed in two steps according to a grounded theory approach. First, broad themes were identified guided by a set of initial sensitizing constructs (Alvesson and Sköldberg, 2000; Bowen, 2006). Following this step, new research questions arose and the research material was coded and categorized, allowing the search for

[1] http://www.lusax.ehl.lu.se/

patterns within and across cases. Emergent patterns were then compared to existing theory and empirical research, in an iterative, abductive process (Eisenhardt, 1989).

The particular empirical data on which we base this paper is derived from a subset of the research efforts described above. However, as we methodologically attempt to take a meta-perspective and present a cross between a longitudinal (on-going) and historical (although recent) case study, we need to draw upon all the experience that we have gained during the research project. Empirically, we focus mainly on a set of (now historical) facts and attempt to unravel a particular episode of disruptive technological change within the electronic security industry, using an actor-network perspective. We finally link and contrast our findings to extant literature and theory in order to hopefully contribute some insights.

Technological change in the video surveillance industry

Introduction

Historically a virtually isolated sector – in terms of technology, products, customers and industry participants – the electronic security industry[2] has for the past decade been facing a technological change as mechanical and analog security products become IT- and IP-network enabled and whole product segments are shifted onto digital technology platforms. Although digitalization affects all sectors in the industry, this case will focus on the video surveillance market, in which the effects of the migration from analog to digital has been particularly appreciable. Today, a USD 10-15 bn market globally, video surveillance is also the security sector with the highest growth rate, at close to double-digit annual growth rates.

To understand the change in the video surveillance industry, it is crucial to gain an understanding of the underlying technologies. From a product perspective, a video surveillance system can be said to comprise three distinct components: cameras, video transmission system, and monitoring and recording. Apart from the introduction of color, the

[2] This industry definition encompasses equipment such as video surveillance, access control, fire and intrusion detection, and associated services such as systems integration and installation.

basic technology of a fully analog video surveillance system has changed little since it first appeared about half a century ago: A camera outputting a PAL or NTSC (standards carried over from broadcast television) video signal is connected through coaxial cable to a monitor and – optionally – to a recording device, traditionally a video cassette recorder (VCR), but today more commonly a digital video recorder (DVR). An analog video surveillance system is by nature a closed system, delimited by the physical cabling inter-connecting all the components. Hence the traditional moniker Closed Circuit TV – which is still widely used (even when referring to modern digital system). Being such a mature technology, based on technological standards set in the 1950s and 1960s, the design and installation of an analog CCTV system is relatively straightforward. According to 'old-timers' in the industry, and as described in CCTV handbooks (e.g. the 'CCTV bible' by Damjanovski, 2005), the most advanced and profession-specific skills of CCTV designers and installers were related to optics, such as selecting and adjusting camera lenses according to available light conditions. The most labour intense part of a typical installation, however involves the running of the transmission and electrical cabling that interconnects individual cameras and the monitoring and recording station.

First wave of digitalization of video surveillance: - enter the DVR

Prior to the advent of the VHS system and affordable consumer-grade video recorders in the late 1970s (Cusumano et al., 1992), recording of CCTV video was rare. With VHS, and so called time-lapse VCRs, which were video recorders developed specifically for CCTV applications, video recording became a mainstream feature during the 1980s, coinciding with the 'rise of CCTV' (Norris and Armstrong, 1999) as seen especially in Britain. Although video cassette recording revolutionized the CCTV industry, the inherent drawbacks of the technology – the poor image resolution, the high failure rate of tapes and VCRs, and not least the hassle of constantly changing and storing tapes – became very apparent over time. By the late 1990s, digital video recording began to emerge as a cost-effective alternative, and by the early 2000s DVRs started to replace VCRs as the recording device in most new CCTV systems. The DVR was designed as a ready-to-use (black) box that could simply replace existing VCRs in a plug-and-play fashion, and in the process drastically facilitate video recording and storage. DVRs were built around a processing unit equipped with embedded, video management software and video capture cards, and with the recorded video being

stored on internal hard drives. Yet – as is the case with consumer DVRs – most of the hassle of parameter configuration has been designed away and hidden from the user's view. Compared to the VCR era, the DVR enabled an install-and-forget type of CCTV system, which greatly strengthened the overall business and user case of video surveillance. Although initially more costly, the increased performance of DVR technology was so apparent to both installers and end users that VCRs became all but extinct in the security industry within a relatively short time, during the early 2000s.

The second wave of digitalization: the age of IT and IP convergence

Whereas the DVR was in all respects based on digital technology, it mimicked the simplicity of the VCR and did not challenge the analog, closed-circuit logic and design of the traditional CCTV system. By the mid-2000s however, the success of digital cameras in the consumer market started to challenge the logic of using analog cameras based on old television standards for CCTV purposes. In response, video surveillance systems based on digital cameras transmitting encoded video bitstreams using an Internet Protocol (IP) over computer networks (using standard Cat 5 twisted pair cabling or even Wifi) emerged as the platform that would thrust CCTV into the all-digital era. By converting video into digital streams that are transported over IP, the closed logic of traditional CCTV systems was broken. Notwithstanding bandwidth constraints, an IP video system can theoretically be monitored by anyone in any location as long as they have access to the Internet. Compared to VCRs and DVRs, which were ubiquitous and well-understood recording standards during their respective CCTV eras, IP video also completely opened up the recording end of the system. In a typical IP video system, DVRs are replaced by network video recorders (NVRs), which are essentially normal PCs equipped with video management software that the handle recording of multiple video streams. However, recording can also be distributed and carried out a the 'edge' of video network, using in-camera recording on SD cards, by recording to network access servers (NAS). Alternatively, the video stream can simply be sent via IP networks to the 'cloud', i.e. to be stored at remote servers hosted by service providers or at a user's central offices. Hence, in the digital world, the flexibility and possibilities in designing a video surveillance system is nearly endless, in stark contrast to the closed logic of analog CCTV systems of the past.

Although a few, albeit important, skills are carried over from the analog world – such as lens selection and camera placement – digital systems tend to use built-in intelligence to auto-configure many parameters that CCTV installers had to manually adjust in the past. In contrast to an analog system, designing and installing an IP camera surveillance system thus primarily involves advanced network, router and server configuration, choosing cameras and server recording equipment based on features such as resolution and video compression codecs, selecting and configuring a digital recording system, and choosing and installing the software needed for control and operation of the system.

Complicating matters further for installers (and end-users) is the fact that in contrast to the traditional CCTV industry, where vertically integrated manufacturers typically provided turnkey CCTV systems, including cameras, cabling, recording equipment and all accessories, network video vendors typically follow the IT industry model of vertical specialization and de-integration (Yoffie, 1997). Hence, IP camera vendors provide only cameras and rely on an 'ecosystem' of other IT players to provide all the different components and accessories needed to for a complete system, such as servers and video management software. This increased complexity puts the onus on the installer or end-user to integrate software and security hardware, which is a challenge compared to the stand-alone, proprietary solutions with integrated software that was the norm in analog CCTV.

Industry effects of the shift to digital

Around 2006-2008, the above described technological shift to digital platforms and IP networking was the all-encompassing concern and talking-point within the security industry. Due to the technological convergence of traditional security and IT, the the IT industry was practically expected to acquire and engulf the relatively small electronic security industry within a few years. These concerns where partly the result of an aggressive push of IT giants such as Cisco and IBM into network video surveillance. Compared to the intensely local and fragmented security industry, consolidated IT giants like Cisco – whose yearly revenues rivaled those of entire segments of the security industry – were feared and revered by the old guard in the security industry. The major IT players quickly became head sponsors of important industry shows, and started massive marketing campaigns directly aimed at security end-users. To the new players coming from what they regarded as the state-of-the-art IT

industry, the security market appeared conservative, old-fashioned and slow-moving, with complacent and high-margin distribution channels and un-sophisticated end-users (e.g. ‘old cops’).

The overall vision – form the IT side – was that the disruptive and inevitable shift to digital would not only shift the supply side of the industry towards IT, but also cause a rapid shift within user organizations. IT departments were expected to become integrated with the security function – at least in larger organizations – or even take over operations of networked systems such as IP video surveillance, thus gradually pushing the security function into the realm of IT decision makers. Similarly, for the lower end of the market, new types of players – such as local IT consultants and specialized IT players (such as point-of-sales systems installers in retail) were gradually expected to replace the old guard of local, IT- and IP-illiterate, security installers, that were likely to resist the shift to digital. Thus within, a few years, significant portions of the industry were expected to have adapted to the superior IT modus operandi.

It quickly became apparent, however, that such bullish visions of rational and disruptive technological change were flawed. Digital technology did certainly make good progress – partly because the industry as whole was experiencing rapid growth – but the rate of the adoption of digital video surveillance was not as high as initially expected. As a result, Cisco and many other large IT players withdrew from the security arena within a year or two. Today in 2011 – a full decade after the first digital video surveillance systems were launched commercially – only about 30-40% of surveillance video systems sold globally are digital, a figure that is even lower when looking at currently installed systems. In some vertical markets, such as retailing where video systems tend to be small and need to be cost-effective, 80-90% of new systems sold are still based on the analog camera and DVR model that became the standard in the early 2000s.

Part of the explanation for this is due to the peripheral role played by security technology in most organizations. Physical security is not a strategic concern – in the way that IT operations are – for a majority companies today, and replacement cycles are normally much longer (5-10 years) than in IT. For new investments and system replacements, there is strong focus on cost,

rather than functionality, which can block technological migration to the latest digital solutions that are typically still more expensive than their analog counterparts. But these are transparent features of the security market, which the IT players were likely aware of when they entered.

Security end-users

While usage of security equipment such as video surveillance today is ubiquitous, pinning down and identifying actual security purchasers and users can be surprisingly difficult. The role of the typical security user can be dispersed within organizations and will depend on factors such as geography and organization size and area of activity. Generally speaking, most large organizations have dedicated security functions, or even departments headed by managers with titles such as security manager or Chief Security Officer (CSO). Security managers have varying and diverse backgrounds, that may include law-enforcement and military experience, facility management, IT and varying technical backgrounds, all depending on the actual appointed role. As there are virtually no formal educational programs available for the role of security manager, it is a profession that is built around diverse learned-in-practice skills and experience built up over long careers. For this reason, security managers tend to be senior in age.

In relation to technology, few security managers today have the in-house competence to design and install their own security systems, including video surveillance. For these tasks, they typically rely on establishing relationships with systems integrators and consultants (see below). Rather than specifying specific technologies, or specific component brands, security managers usually specify the type of solution and features they need, leaving it up to systems integrators or consultants to to decide system design and component selection. Establishing good working relationships with trusted system integrators and consultants is an important concern for security managers. Another important aspect that relates to technology is that security work and security managers are largely guided by the sensibilities and culture of high reliability organization (HRO) (Weick, 1987; Roberts, 1990). HRO puts an emphasis on maintaining error-free operations in times of crisis, which for security managers translates into an obsession with reliability of the equipment used, and a need to feel “in control” of the technology at one’s disposal. What matters is thus not the latest features or being at the

frontier of technology, but rather that things work when they are supposed to, and with a minimum of maintenance and downtime.

As security professionals, even within larger organizations, typically have no or only a few colleagues, formal and informal communities of practice play a very important role as fora where security managers meet and share experiences, head-hunt and recommend jobs to each other, and socialize. The largest professional organization for security professionals is ASIS International, formerly American Society for Industrial Security, but today global in its scope. With the aim of professionalizing the sector, ASIS organizes a multitude of industry events including a yearly US-based industry attended by "everyone" in the industry, as well as a large number of local education and certification programs around the world. Many other formal security communities of practice are formed regionally and internationally, as well as around particular technologies, including user-groups focused on specific vendor platforms. Experienced security managers also tend to have wide-ranging personal networks encompassing e.g. local law enforcement, private investigators, other security managers as well as systems integrators and consultants. Thus, belonging to several, highly networked 'communities of practice' within security can be seen as requirement, at least for senior security managers.

Outside the realm of larger organizations, however, the vast 'lower-end' of the market made up of smaller firms and small businesses such as retail outlets is essentially 'user-less' in the sense that security is purchased and used by people who are not specifically responsible for a dedicated security function. In these cases, security can be seen as an operational 'hygiene factor', like cleaning services and building maintenance, and is typically sourced locally, even in the case of multinational firms or retail chains. Local installers and security integrators play an important role in furnishing such customers with appropriate security solutions and services, including taking care of the red tape often involved in getting local permits to install a surveillance video system. Again, the user typically buys a video surveillance 'solution' and it is nearly always the security installer that decides what type technology and components to use.

Complicating the user picture further, independent security technology consultants also play a very important role in the market in terms of selecting technology platforms. Consultants typically work alongside security managers in larger organizations, or take the role of a 'proxy' user in smaller organizations that lack a dedicated security function. The typical role of a consultant is to design and specify security systems, and to assist the user in assessing bids from installers and integrators. Not all user employ consultants, as some resourceful security managers do their own design and specification work. In the lower-end of the market, where system design is more trivial, installers and integrators often incorporate the consultants' tasks as part of the job.

Discussion

To some extent, the technological change in the security industry as described above follow an overarching deterministic path. No industry has successfully resisted a change from analog to digital technology, except for a few pockets of resistance.[3] From nearly all aspects, digital technology is superior and more flexible than analog, even if this comes at a cost premium, at least initially. In fact, security is probably one of the few technology industries that have not yet already made the leap. So what explains the slow rate of the migration from analog to digital and the fact that, despite the apparent disruptiveness and increased performance of digital technologies, industry entrants from the IT side have by and large not been able to break up the traditional channels and strong structures that have been built up in the security industry over the past decades? And why, in contrast, did the shift from VCRs to DVRs, which represented the first wave of digitalization of video surveillance, happen almost overnight?

To answer these questions, it is necessary to look at the nature of the technological systems in question as well as the social networks in which they are sold, implemented and used. As we have seen above, the use of video surveillance within the security experienced a boom in the

[3] Where such resistance has usually been based on aesthetic or nostalgic concerns, such as the continued use of vacuum tubes in place of solid-state electronics in audio and instrument amplifiers.

late 1970s and the 1980s with the advent of the VCR, allowing the recording of CCTV footage for later review. Over the course two decades, the analog camera and VCR model became the ubiquitous 'dominant design' for a video surveillance system. In ANT terminology, the design of a video surveillance system became a 'black box', in the sense that there were no alternative technologies and thus no controversies to be settled. Given the nature of security work, and end-users HRO sensibilities, there is also an inherent demand for products that are as 'black-boxed' as possible, i.e. that they work reliably and are easy use and maintain. The same also holds for security installers and consultants. As explained earlier, the installer/consultant often takes on the role of proxy user, when a security manager or security purchaser is illiterate in technology. As their local reputation is important, installers and consultants need to deliver robust solutions, which often means sticking to what has worked well in the past. What emerges is thus a picture of the pre-2000s analog video surveillance industry as a stable actor-network, with users and industry participants strongly aligning and associating themselves with a 'black-boxed' technology platform.

Seen in the light of this actor-network, the successful and uncontroversial replacement of the VCR with the DVR is easy to understand. Over time, the VCR emerged as the weakest link of the CCTV system, making the benefits of the DVR apparent, despite an initial higher cost. More importantly however, the DVR did not challenge the overall logic of the 'black boxed' CCTV system. Rather, it could simply replace existing VCRs in a plug-and-play fashion. From an industry perspective, no resistance was mounted from the manufacturers of security VCRs, who saw the CCTV market as a marginally interesting niche market, and whose 'association' (in ANT terms) with CCTV had consequently always been weak. For integrators, installers, consultants and users, the DVR did represent some new learning challenges, but never to the point of having any de-skilling or 'competence-destroying' effects. What happened was rather that the overall business and user case of video surveillance was further strengthened through the introduction of the robust DVR recorder, representing what Tushman and Anderson (1986) would call a 'competence-enhancing' change. By keeping the underlying logic of the CCTV actor-network intact, the DVR simply made the 'black box' even blacker and stronger than it was before.

In contrast, the push towards all-digital video surveillance in the mid-2000s put the security industry under intense pressure to open its analog 'black boxes' and reconfigure long-established networks from the ground up. The initial reaction was that the industry was on the brink of a major digital disruption, that would soon lead to the wholesale replacement of analog with security technologies. For industry outsiders, such as people from the IT industry, this deterministic digital evangelism seemed logical and sound: those who were reluctant or unable to change and tried to resist the surge of superior digital technology and IT practices, where likely to face the effects of an industry-wide Darwinian cleansing.

The initial strategy of the IT industry giants entering the industry, was to use their mighty influence to accelerate this disruption as much as possible. The IT and IP-based security entrants thus engaged in a fierce rhetorical war on the old ways, where the basic premises of security work was redefined and linked to IT security and IT technologies. The IT players thus sought to transform the industry through processes of 'translation', where security technology became intrinsically linked to – or converged – with IT systems on many levels: video over IP networks, integration with IT security, and the importance of breaking the organizational silos between security departments and IT departments (where e.g. Cisco had armies of loyal end-user adherents).

However, the black-boxed notion of CCTV and the socio-technical networks of the security industry proved to be much more resilient to disruptive change than the IT entrants had expected. Both users and the incumbent security industry realized the potentially competence-destroying effects of IT, and soon launched their own 'anti-programs'. The most effective of these anti-programs was simply to remain passive, and go about doing business as usual, slowly adopting new technology in a more comfortable pace. Security managers also bonded together in their communities of practices, where resentment towards the arrogance and exaggerated rhetoric of the IT players grew strong, mediated by private exchanges of anecdotes of botched IT-related security projects and similar 'horror stories', in which the introduction of supposedly 'cutting-edge' IT and IP technologies turned out to be 'bleeding-edge'. The "deploy-and-pray" culture prevalent in IT, where new systems with novel features are launched without extensive testing and eventual problems are patched as they appear, clearly was not compatible with the HRO sensibilities of security users. The incumbent

security industry was quick to latch onto these sentiments, promoting a slower, safer and smoother transition to new technologies, by way of e.g. hybrid analog-digital solutions. Faced with this resistance, the IT giants made little headway into the market and soon withdrew almost completely, at least for the time being.

It should however be noted that empirical example shows that security users are not opposed to technological change per se, as witnessed in the successful shift from analog VCR to digital DVR technology. Rather, it appears that implementing new technology successfully in the security industry, one must not try to transform existing socio-technical networks too rapidly. Following their HRO sensibilities, security users are interested in reliable function, not technology or 'features' per se. This has had to be learned the hard way by the vendors of IP cameras who – deterministically – have for years been touting the intrinsic superiority of digital technology. Only recently have they learned to see things from the user's perspective, and to translate and attach aspects of the new technology to factors that actually matter to users. As shown by Pinch (2008) in his study on Moog vs. Buchla, on the 'closure' of the dominant design of the synthesizer, users are crucial in institutionalizing new technology. By engaging with users, witnessing them interact with his designs, and changing them when necessary, Moog managed to make a successful translation, linking the acoustic keyboard tradition with the electronic synthesizer.

Consequently, faced with the powerful 'black box' of analog-DVR CCTV system, and the general reluctance to rapid change among security users, IP camera and video system vendors have had to change their rhetoric several times, in order to re-translate the benefit of going all digital to end-users. Initially, the remote monitoring (being able to watch your surveillance cameras from anywhere) aspects were highlighted. As this proved useful only to smaller segments of the market, and could also be accomplished with a DVR, the IP camera vendors shifted to touting the superior megapixel and high definition picture quality of digital cameras. While analog video has to stick to age-old television standard resolutions, digital cameras have no restrictions, putting no upper limit on picture quality other than prohibitive cost. Finally, realizing that expensive HD cameras were not successful in breaching the difficult market of small camera installations, the rhetoric has just recently shifted again. This time to lower-cost IP cameras with on-board intelligence, enabling cloud-based recording,

eliminating the need for using a central recording unit such as a DVR. Having finally learned the lesson that security users always tend to migrate to the most simple and black-boxed solutions, this could perhaps be the technology model that finally breaks the dominance of the DVR model.

Conclusions

This paper has argued that it is important to adopt a user perspective in order to gain an understanding of technological change. The empirical study shows how established industry socio-technical actor-networks encompassing users, consultant, channels and manufacturers collectively can resist disruptive attempts of technological change from powerful outside forces. In the security industry such networks have developed over time, in reflection of end-users need for simple and highly reliable systems. The empirical example shows how networks formed around communities of practice that span formal organizational boundaries can be important in shaping use and adoption of new technology. Collectively, through participation in these communities of practice, users defended their profession and organizational status from the competence-destroying effects of too rapid and sweeping shifts in technology.

In this respect, there interestingly appears to be a strong correlation between the strength of security communities of practice and the professional identity of security managers and the resistance to digitalization. The US and UK consistently show a significantly lower industry adoption of digital technology compared to most European countries where the security profession is not as well-organized, and where security management culture is weaker and more diffused within organizations. This mirrors the results reported by Eriksson-Zetterquist et al. (2009), where purchasers were shown not to be strong enough as a professional group to resist the change imposed by a new electronic purchasing system.

The video surveillance case also highlights the importance of understanding technological artifacts the the role they play in socio-technical networks. The traditional CCTV system,

represented by the black-boxed assemblage of analog cameras and DVRs is good example of technology being reified into an path-dependent institution, exhibiting strong associations to a heterogenous actor-network made up of manufacturers, installers and users. Even in the face of 'superior technology', such strongly aligned actor-networks are hard to break-up, especially when the professional 'survival' of its participants is at stake.

It appears then, that users matter in times of technological change. It also appears that user groups that from a casual glance appear weak, powerless and isolated can use their extended networks and communities of practice to resist technology. To uncover and describe such 'transcendental' social networks between people and technology that lie beyond formal structures, an actor-network perspective can be very helpful.

References

Adner, R. (2002). When are technologies disruptive? A demand-based view of the emergence of competition. *Strategic Management Journal*, 667-688.

Alvesson, M., & Sköldberg, K. (2000). *Reflexive methodology: New vistas for qualitative research*. Sage Publications Ltd.

Anderson, P., & Tushman, M. L. (1990). Technological Discontinuities and Dominant Designs: A Cyclical Model of Technological Change. *Administrative Science Quarterly*, 35 (4), 604-633.

Arthur, B. W. (1989). Competing technologies, increasing returns, and lock-in by historical events. *The Economic Journal*, 99(394), 116-131.

Arthur, B. W. (1990). Positive feedbacks in the economy. *Scientific American*, 262(2), 80-85.

Barley, S. R. (1986). Technology as an Occasion for Structuring: Evidence from Observations of CT Scanners and the Social Order of Radiology Departments. *Administrative Science Quarterly*, 31(1), 78-108.

Barley, S. R. (1990). The Alignment of Technology and Structure through Roles and Networks. *Administrative Science Quarterly*, 35(1, Special Issue: Technology, Organizations, and Innovation), 61-103.

Bowen, G. A. (2006). Grounded theory and sensitizing concepts. *International Journal of Qualitative Methods*, 5(3), 1-9.

Brown, J. S., & Duguid, P. (1991). Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation. *Organization science*, 2(1), 40-57.

Callon, M. (1986). Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay. In J. Law (Ed.), *Power, action and belief: A new sociology of knowledge?* (pp. 196–233). London: Routledge and Kegan Paul.

Callon, M. (1991). Techno-economic networks and irreversibility. In J. Law (Ed.), *A sociology of monsters: Essays on power, technology, and domination* (pp. 132-161). Routledge.

Christensen, C. M. (1997). *The innovator's dilemma: when new technologies cause great firms to fail.* Harvard Business School Press.

Constant, E. W. (1987). The social locus of technological practice: community, system, or organization. In W. E. Bijker, T. P. Hughes, & T. J. Pinch (Eds.), *The social construction of technological systems: New directions in the sociology and history of technology* (pp. 223–242). Cambridge, MA: MIT Press.

Cusumano, M. A., Mylonadis, Y., & Rosenbloom, R. S. (1992). Strategic Maneuvering and Mass-Market Dynamics: The Triumph of VHS over Beta. *The Business History Review*, 66 (1), 51-94.

Damjanovski, V. (2005). *CCTV: Networking and Digital Technology* (2 ed.). Burlington, MA: Elsevier Butterworth-Heinemann.

Dodge, M., & Kitchin, R. (2005). Code and the transduction of space. *Annals of the Association of American geographers,* 95(1), 162-180.

Dosi, G. (1982). Technological paradigms and technological trajectories. *Research policy*, 11 (3), 147-162.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, 532-550.

Edmondson, A. C., Bohmer, R. M., & Pisano, G. P. (2001). Disrupted Routines: Team Learning and New Technology Implementation in Hospitals. *Administrative Science Quarterly*, 46(4), 685-716.

Eriksson-Zetterquist, U., Kalling, T., & Styhre, A. (2011). *Organizing Technologies*. Malmö: Liber.

Eriksson-Zetterquist, U., Lindberg, K., & Styhre, A. (2009). When the good times are over: Professionals encountering new technology. *Human Relations*, 62(8), 1145-1145.

Fox, S. (2000). Communities Of Practice, Foucault And Actor-Network Therory. *Journal of Management Studies*, 37(6), 853-868.

Granovetter, M. (1985). Economic Action and Social Structure: The Problem of Embeddedness. *The American Journal of Sociology*, 91(3), 481-510.

Greener, I. (2002). Theorising path-dependency: how does history come to matter in organisations? *Management Decision*, 40(6), 614-619.

Henderson, R. M., & Clark, K. B. (1990). Architectural Innovation: The Reconfiguration of Existing Product Technologies and the Failure of Established Firms. *Administrative Science Quarterly*, 35(1, Special Issue: Technology, Organizations, and Innovation), 9-30.

Hughes, T. P. (1986). The Seamless Web: Technology, Science, Etcetera, Etcetera. *Social Studies of Science*, *16*(2), 281-292.

Hult, J. (1992). The Itera Plastic Bicycle. *Social Studies of Science*, 22(2), 373-385.

Kuhn, T. S. (1996). *The structure of scientific revolutions* (3 ed.). University of Chicago Press.

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society.* Cambridge, MA: Harvard University Press.

Latour, B. (1991). Society is technology made durable. In J. Law (Ed.), *A sociology of monsters: Essays on power, technology, and domination* (pp. 103-131). Routledge.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory.* Oxford University Press, USA.

Law, J. (1992). Notes on the theory of the actor-network: ordering, strategy, and heterogeneity. *Systemic Practice and Action Research*, 5(4), 379-393.

Lawson, C. (2007). Technology, technological determinism and the transformational model of technical activity. In *Contributions to Social Ontology* (pp. 32–49). London: Routledge.

Leonard-Barton, D. (1992). Core Capabilities and Core Rigidities: A Paradox in Managing New Product Development. *Strategic Management Journal*, 13, 111-125.

MacKenzie, D., & Wajcman, J. (1999). *The social shaping of technology* (2 ed.). Maidenhead: Open University Press.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: The rise of CCTV*. Oxford: Berg.

Nowotny, H., Scott, P., & Gibbons, M. (2003). *Introduction: Mode 2 Revisited: The New Production of Knowledge*. Minerva, 41(3), 179-194.

Nye, D. E. (2006). *Technology matters: questions to live with*. The MIT Press.

Oudshoorn, N., & Pinch, T. (2003). Introduction: How Users and Non-Users Matter. In N. Oudshoorn & T. Pinch (Eds.), *How users matter: The co-construction of users and technology* (pp. 1-25). Cambridge MA: The MIT Press.

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other. *Social studies of Science*, 14(3), 399-441.

Pinch, T. (2008). Technology and institutions: Living in a material world. *Theory and Society*, 37(5), 461-483.). The MIT Press.

Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. *Organization Science*, 1(2), 160-176.

Romer, P. M. (1990). Endogenous Technological Change. *The Journal of Political Economy*, 98(5, Part 2: The Problem of Development: A Conference of the Institute for the Study of Free Enterprise Systems), S71-S102.

Steen, J., Coopmans, C., & Whyte, J. (2006). Structure and agency? Actor-network theory and strategic organization. *Strategic Organization*, 4(3), 303-312.

Taylor, A., & Vincent, J. (2005). An SMS History. In L. Hamill, A. Lasen, & D. Diaper (Eds.), *Mobile World* (pp. 75-91). Springer London.

Todd, E. N. (1992). Electric Ploughs in Wilhelmine Germany: Failure of an Agricultural System. *Social Studies of Science*, 22(2), 263-281.

Tucker, C. (2008). Identifying Formal and Informal Influence in Technology Adoption with Network Externalities. *Management Science*, 54(12), 2024-2038.

Tushman, M. L., & Anderson, P. (1986). Technological Discontinuities and Organizational Environments. *Administrative Science Quarterly*, 31(3), 439-465.

Weick, K. E. (1987). Organizational Culture as a Source of High Reliability. *California management review*, 29(2), 112-127.

Wenger, E. C., & Snyder, W. M. (2000). Communities of practice: The organizational frontier. *Harvard Business Review*, 78(1), 139-146.

Williams, R., & Edge, D. (1996). The social shaping of technology. *Research policy*, 25(6), 865-899.

Yates, J. (2006). The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology/How Users Matter: The Co-Construction of Users and Technologies. *Business History Review*, 80(1), 144-147.

Yoffie, D. B. (1997). Introduction: CHESS and competing in the age of digital convergence. In D. B. Yoffie (Ed.), *Competing in the age of digital convergence* (pp. 1-36). Boston, MA: Harvard Business School Press.