Chasing Shadows: Control, Virtuality and the Production of Trust
David Knights, Faith Noble, Theo Vurdubakis and Hugh Willmott
Organization Studies 2001; 22; 311
DOI: 10.1177/0170840601222006

The online version of this article can be found at:
http://oss.sagepub.com/cgi/content/abstract/22/2/311

Published by:
http://www.sagepublications.com

On behalf of:
European Group for Organizational Studies

Additional services and information for Organization Studies can be found at:

Email Alerts: http://oss.sagepub.com/cgi/alerts

Subscriptions: http://oss.sagepub.com/subscriptions

Reprints: http://www.sagepub.com/journalsReprints.nav

Permissions: http://www.sagepub.co.uk/journalsPermissions.nav

Citations http://oss.sagepub.com/cgi/content/refs/22/2/311
Chasing Shadows: Control, Virtuality and the Production of Trust*

David Knights, Faith Noble, Theo Vurdubakis, Hugh Willmott

Abstract

In recent years, the topic of trust has become the focus of renewed attention in organizational theory and research and, in particular, where electronic distribution and associated ‘virtual’ forms of organizing are prevalent. The question of trust, always an issue in financial transactions, is exacerbated the more the physical element is removed. The paper focuses on the issue of trust as it currently appears in the newest of these distribution channels, online and Internet financial services, and smart cards. In both theory and practice, notions of trust are often opposed to concepts such as power or control, and are deployed as part of a dualistic either/or proposition. Drawing on ongoing research in the financial services sector, the paper attempts a more nuanced exploration by focusing on attempts to ‘manage’ trust, the problems such attempts encounter, the various techniques employed in their resolution and the power relations in which they are embedded.

Descriptors: identity, power and control, security, trust, virtuality

Introduction

Issues of trust have recently become the focus of renewed attention in organizational theory and research (Kramer and Tyler 1996; Lane and Bachman 1998), as well as in numerous attempts to understand social relations more broadly (Fukuyama 1995; Giddens 1990; 1992; Gambetta 1988). This academic interest has been further stimulated by the growth of non-face-to-face, computer mediated forms of communication and commerce, where trust tends to become identified as a key, if problematic, issue by designers and users. The ‘problem of trust’ is widely seen as co-extensive with the increasing usage of electronic media of networking and delivery, which in many sectors are complementing and perhaps even replacing more established, methods of business dealings. In the context of an advancing ‘virtualisation’ of financial transactions through the use of online, internet and ‘smart card’ facilities, sensitivity and increased attention to possibilities of fraud and error is perhaps to be expected — even though expert opinion remains divided on the subject.

Drawing on our research in financial services, we explore how problems of trust are being ‘managed’, especially in relation to matters of control,
with the proviso that we do not view these two concepts in a dualistic fashion, as polar opposites. Rather, our perspective examines how the problems of control and of managing trust often share a common platform. The production of trust often relies on, and reproduces, relations of control because control also becomes problematic in the absence of trust. We are concerned, therefore, not just with the various techniques employed in the resolution of perceived problems of trust, but also with the power relations in which trust relations are embedded. The central focus of the paper, however, is on how trust is constructed and managed in the process of introducing virtual forms of trading.

### Conceptualizing Trust

Surveys of social science research on trust have periodically lamented what Lewis and Weigert (1985: 975) identify as ‘a good deal of conceptual confusion regarding the earning of trust and its place in social life’ (see also Misztal 1996). Social theories and research do indeed tend to deploy the concept of trust in diverse and often contradictory ways. For instance, ‘trust’ has often been identified as the ‘Other’ that is marginalized and excluded in the operation of calculative economic reason (Hutton 1997: 30–32; Richardson 1972). For some authors, however, trust is construed as an integral lubricant of economic exchange; and, therefore, is understood to be co-extensive and synonymous with an economizing logic (Axelrod 1997; Coleman 1990; Hofstadter 1985). In Fukuyama’s (1995) influential thesis, the concept of trust is presented as a basis for distinguishing between national cultures that are readily differentiated within a twofold typology. A ‘high trust’ culture is deemed to confer competitive advantages upon the economies of Japan, Germany, or (decreasingly) the United States, whereas the opposite is the case for ‘low trust’ countries such as Italy, China or France. In turn, this thesis is contradicted by other, equally often, cited assessments of the role of trust in economic performance (e.g. Sabel 1992; Piore and Sabel 1984). Similarly, much of what Fukuyama cites as evidence of high trust has been denounced by (western) commentators as manifestations of an entrenched culture of corruption, during Japan’s recent spell in the economic doldrums (e.g. Leadbeater 2000: 164–166).

In recent years then, much intellectual effort has been dedicated, and academic ink shed, in the cause of constructing and refining classifications of the phenomenon of trust and of precisely mapping out its role in social relations (e.g. Lewicki and Bunker 1995; Sako 1992). It is not our intention to add further attempts at providing a comprehensive survey of proliferating theoretical perspectives and empirical studies of trust. Nor do we aspire to ‘cut through’ them so as to ‘grasp the essence’ of the subject (Misztal 1996: 13; Leadbeater 2000: 158). Instead, our focus is to examine the ways in which the language of trust is deployed to ‘problematize’ — in Callon’s (1986) sense of the term — particular events or situations. In this respect, we can identify a number of interconnected themes running
through most discussions of trust that are of particular relevance to our
analysis of developments in financial services. By construing trust as a
means for coping with the freedom or indeterminacy of other agents, much
contemporary discussion of trust tends to evoke the so-called ‘Hobbesian
problem’ of order. This is the ‘paradox’ as it is put (e.g. Hollis 1998: 1–25),
of orderliness in a society of otherwise free and self-interested subjects.
The quest for the mechanisms that prevent chaos and indeterminacy, and
impose order and structure in human affairs came to be seen, after Parsons
(1951), as the task of social science, or, as recently reformulated by Giddens
(1990:14) and other theorists of modernity, the search for those mecha-
nisms which ‘bind time and space’ together to constitute organization and
society as we know them. Whether explicitly or by implication, academic,
journalistic and practitioner discourses on trust tend to involve the (re)artic-
ulation and elaboration of this ‘problem of order’. Explicitly, we can see
this in the case of Luhmann’s (1979) thought experiment with a totally
unstructured, shapeless and entropic imaginary world as the Other, against
which the real world with its evident stabilities can be contrasted and its
mechanisms of co-ordination held up to scrutiny (see also Fukuyama 1996:
iiix; Misztal 1996). By implication, it occurs when the grand problem of
order is small changed into questions as to how and under what circum-
stances social actors can be expected not to exploit trust (e.g. Dasgupta
1988; Axelrod 1997).

All organization depends on trust, according to Drucker (1990), and ‘trust
is mutual understanding. Not mutual love, not even mutual respect.
Predictability (ibid. 89, emphasis added). For instance, in Luhmann’s
(1995) influential revision of Parson’s systems theory, trust and distrust are
functionally equivalent strategies for dealing with what he terms the prob-
lem of ‘double contingency’: where counterfactual trust has to be granted
(and vulnerability thereby exposed), or withheld, in advance of it being
confirmed. In other words, trust/distrust constitute relevant responses to ‘sit-
uations where one must enter into risks one cannot control in advance —
or forced to refuse participation’ (Luhmann 1995: 129). The attempt to
‘control in advance’ through the exercise of power, (when this option is
available to the actor), is, in this sense, an alternative means of influenc-
ing ‘the selection of actions in the face of other possibilities’ (Luhmann
1979: 112). In this view, ‘trust’ — which signals a vulnerability of trustor
to the actions of the other, the trustee — and ‘power’ — which attempts
to control the actions of the other — are both alternative social mecha-
nisms for resolving problems of order and organization.
At the same time, ‘trust’ and power-assisted ‘control’ are morally charged
categories. While respect for the autonomy of the other is held to charac-
terize trust, mechanisms of control are viewed as the operationalization of
Within studies of work and organization, for example, trust has commonly
been identified as a feature of systems that posit an alternative to Taylorist
and Fordist systems of control (Fox 1974; Ritzer 1993; Hirst and Zeitlin
1991). In contrast to methods and systems that rely on close supervision
or ‘direct control’, trust is understood to underpin more ‘democratic’ styles of leadership, or philosophies of managing, that engage the relative autonomy of the employee (Friedman 1977). Such approaches are often associated with mentoring and coaching in which employee discretion and creativity is celebrated and promoted. A long tradition of management thought conceptualizes trust and control as opposing alternatives. From McGregor’s (1960) distinction between theories X and Y, to the current preoccupation with the opposition between bureaucratic and (post-bureaucratic) flat, ‘non-hierarchival’ organization — this trust/control opposition is invoked and re-worked (Peters 1988; Moss-Kanter 1996). Nevertheless, to view ‘power/control’ and ‘trust’ as polarized rather than interdependent can be potentially misleading. Even when practices and relationships appear to be based upon trust rather than control (as in the case of the professions), there is often implicit reliance on systematic controls. These controls are integral to processes of education and professional socialization, where neophyte professionals are expected to embrace certain self-disciplining protocols. In this example, control is a condition of, and is entwined with, rather than standing in opposition to trust. Conversely, even in a situation where supervision is close, any relationship short of slavery depends upon the trust invested by — for instance — the employee in the employer, that contractual obligations will be honoured and that wages will be paid at the end of the week (Luhmann 1979). Such trust is vested in an (ideologically embellished) confidence in the reliability of established practices and institutions (Ezzamel and Willmott 1992). After all, as Gambetta (1988) notes, even the Mafia has recourse to notions of trust.

In this respect, an analytical distinction is often drawn between, on the one hand, (inter)personal trust and on the other, institution based trust (Zucker 1986). Most studies of trust at work — and more broadly in principal–agent relations — would, in this view, share a preoccupation with interpersonal trust. However, the argument goes, personal interaction is no longer the main or most significant means of trust production. In Giddens’ (1990; 1992) well-known re-working of Luhmann’s approach, modernity is understood to involve a qualitative shift in the basis of trust relations. Reliance upon abstract/expert systems, with the role of the trustee increasingly taken by ‘anonymous others’, is seen to supplant trust secured by bonds of kinship, community or tradition. In this context, individual social actors are viewed as ‘access points’ or interfaces between various abstract systems and the general public. For instance, the trust placed in a professional, such as a doctor (the group people are most likely to trust according to MORI 1998: 32, or a pilot, or for that matter a government official), represents trust invested in institutionally certified and enforced standards of conduct or expertise. At the same time, the face-to-face mode of the relationship helps to humanize and ‘re-embed’ a system in interpersonal interaction, thus rendering it trust-worthy. There is, one might say, a relationship of supplementarity between person and system. No institution can remain trusted without the continual reproduction of trust through interpersonal relations. However, the latter is facilitated by a reputation of trust at the
institutional level. There is therefore much in this work which is consistent with an understanding of the production and maintenance of ‘trust’ as itself closely related to particular systems of power and control. In practice, it is often impossible to disentangle trust invested in specific people from trust placed in institutional mechanisms. Buying from, or working for a company entails ‘interpersonal’ and ‘institutional’ dimensions of both trust and control.

Within the relationship between the providers of services and their customers, diverse systems of control have been developed, at least in part, in order to gain customers’ confidence and trust. There are clearly important and relevant differences between the employee–employer relationship and this has been the classical, modernist site of work and organization studies and an emergent, postmodern focus on the producer–customer relationship. Alternatively, it is also equally possible to exaggerate the significance of these differences, whereupon parallels and continuities become marginalized or overlooked. A common thread running through relationships of employment and distribution is that each seeks to construct, ‘enroll’, and ‘mobilize’ (Callon 1986) a compliant employee/customer. Both presuppose and require the control of forms of conduct that are deemed unproductive or undermining of relations of trust. While ‘soldiering’ and other forms of ‘slacking’ and ‘skiving’ are the primary forms of behaviour targeted by management control systems, in the provider–customer relationship, the focus is on the effective exclusion of pranksters, fraudsters and defaulters. These stretch along a continuum from close, detailed supervision through the requirement to apply predetermined rules to the trained exercise of professional judgement.

It is relevant to recognize, however, that systems of control designed principally by managers may also provide a valued degree of predictability and security for employees. In this respect, it is not fanciful to talk about employees who place their trust in time and motion studies, and in technological monitoring systems perceived as sources of objective auditable data. They do so precisely because these systems are viewed as being more trust-worthy than other methods, and ‘a protection against unfair work distribution or accusations of dereliction’ (Mason et al. 1999: 14; Bloomfield and Coombs 1992). In this sense, such work control systems are not dissimilar to the security systems in financial transactions that record transactions and exclude unauthorized others from gaining access to private bank accounts.

However, it could be argued that while employees are rendered visible and subject to (inter)personal surveillance of performative behaviours, customers are engaged in remote transactions where only identity, not performance, is checked. Nevertheless, this would be only part of the story. Firstly, it is relevant to note that employers are becoming increasingly interested in specifying the content, and influencing the formation, of employee identity — for example, affinity with corporate values — and not just with whether an individual performs a task to a required standard. Second, the behaviour and performance of individuals as consumers, and not just their
identity, is increasingly a target of technological devices such as credit scoring systems or smart cards (Leyshon and Thrift 1998). The IT enabled knowledges and practices of data profiling, credit rating or ‘forensic marketing’, promise ready access to those whose behaviour suggests that they are acceptable risks, or good prospects for a sale (ibid). In fact, for certain chroniclers of postmodernity (e.g. Deleuze 1992) practices of this kind herald the dawn of a ‘society of control’ where:

‘Marketing is now the instrument of social control and produces the arrogant breed who are our masters. Control is short term and rapidly shifting, but at the same time continuous and unbounded, whereas discipline was long term, infinite and discontinuous.’ (1990:18)

Such apocalyptic vocabulary conveys a picture in which trust has no place (is mis-placed) and where subjects are reduced to a ‘set of codes’ or passwords (ibid). It is, of course, highly questionable whether this is indeed the best way to interpret current developments. At the same time, it is a reminder of the ability of IT to engender ‘extraordinary degrees of optimism and pessimism’ (Woolgar 1998: 336) which, in turn, are expressed in equally forceful language. Thus, the information technology revolution is said to herald a society of leisure and plenty or instead, a society of unemployment and exclusion; the Internet to constitute a utopian space of free communication equality, democracy or, alternatively, the global lair of pedophiles, neo-nazis, cybercrooks and superhighwaymen. The clash between, what we might call, the Roussesque and the Hobbesian visions of ‘cyberspace’ is reflected in current debates about the role of trust and power/control in the new ‘virtual society’. This is the topic we turn to next. However, it is worth recalling an observation made by Fox (1974: 66–67) at this point. In a discussion about exchange and trust dynamics, a difference is noted between formal definitions of trust and everyday usage. Fox gives the example of the resigned lament of parents who, suspicious of the intentions of their daughter’s boyfriend, conclude that ‘We will just have to trust her’, or the veiled threat voiced by a kidnapper to his victim: ‘You just have to trust me’. Yet in both cases, trust is ‘conspicuously absent’. Rather than condemn such usage as illogical or at odds with the ‘nature’ of trust (e.g. Leadbeater 2000: 158–1620, we might see it as particularly relevant to our discussion.

Trust and the Virtual Marketplace

Since 1997, the UK government and, in particular, the Prime Minister has repeatedly assured the business community of its commitment to making ‘the UK the best environment for electronic business by 2002’ (e.g. DTI 1999a: 5). Between conception and execution, however, falls the shadow of the ‘digital looter’. Evidence has been accumulating that the vision of the virtual marketplace is under threat from a lack of public trust. The perception is that the media of electronic commerce are insecure and wide
open to abuse by fraudsters and pranksters. Retail transactions are seen as being particularly vulnerable. According to the BBC’s *Money Programme* (1999), 93 percent of British consumers do not feel secure when submitting financial details over the Internet (see also Parkinson 1999: 27). As the International Chamber of Commerce puts it: ‘Cybercrime represents a growing threat to e-commerce and its development. It is becoming a major obstacle to companies in building the trust they need in order to succeed in this new domain’ (ICC 1999). In the United States, widely viewed as being ‘ahead’ of the United Kingdom in matters of electronic retailing, while the Internet represents only 2 percent of VISA’s total business, it involves 50 percent of its disputed credit-card transactions (Waring 1999; BBC 1999; Parkinson 1999: 27). At the same time, 7 percent of US Internet shoppers claim to have been the victims of Internet fraud (*ibid.*). In the United Kingdom, the Consumer Association’s *Which?* (1998) on-line survey found that 81 percent of all respondents had never bought anything on the Internet, with nearly half of the respondents citing the fear of fraudulent practices as the reason. Similar results were obtained by a MORI (1998) survey of five countries including the United States and the United Kingdom. Similarly, 69 percent of the companies participating in the UK Department of Trade and Industry survey, ‘cited security as a major inhibitor to purchasing across the Internet’ (DTI 1999b). In a survey of UK financial services (Centre for the Study of Financial Innovation 1998), the issues of security were perceived by the sector to be the biggest obstacle to the take-up of the Internet. Almost all respondents mentioned it, and it received the highest mean ranking. The same theme also emerged from answers to other questions about Net insecurity and the need for strong encryption. (In response to such concerns, the Halifax recently had to withdraw its Internet share buying facilities because of breaches of security [FT, 30/11/99: 4]). Nevertheless, ‘the consensus among the techno-literati is that Net security is a problem of perception rather than of fact’ (CSFI 1998; emphasis in original; see, however, Wallich 1999: 21).

This view is shared by the respondents from our own primary research. As a manager in a major telephone banking operation put it:

‘... at the end of the day, if it’s got a telephone line it could be attacked, but it’s just opening up the attack points very widely and overtly to a much wider audience so that’s all I’ll say, so it’s not actually that that bothers me the most, it’s the perception of security. The perception of security is the biggest issue. So we are here as a bank, we are taking the bank’s good name out there, we are going to provide you with an application. Do I at the same time want to be risking your perception of PC banking forever by a scare story that pops out in the Internet? At the moment the answer is no. ... and that is the biggest issue ... the perception of security.’ (emphasis in original)

It is easy to see how the vocabulary of trust and distrust constitutes a handy tool for conceptualizing the problem of security in virtual markets as well as its remedies: What the virtual marketplace is said to suffer from, is a deficiency of trust. Tried and tested solutions no longer work. Cyberspace escapes or evades legal control (e.g. Tsang 1999). This renders legal norms
and sanctions ineffective. Yet, according to Luhmann (1979), legal norms and sanctions constitute efficacious mechanisms for containing the risk, thus providing would-be trustors with ‘good reasons’ for investing in trust relations. Therefore, in order to remedy any potential deficiency, the task of the various corporate actors is to come up with novel legal, social or technical mechanisms of control and trust production.\textsuperscript{4}

Clearly the issue of trust is of particular centrality to financial services. Any discussion, from whatever disciplinary perspective (accounting, economics, or sociology), of financial practices, firms and institutions is, eventually, bound to touch upon issues of trust. Indeed, financial services can be said to be in, or even to be, \textit{the} business of trust. The creation and maintenance of trust relations is a fundamental condition of their existence.\textsuperscript{5}

Two aspects of the operation of trust relations in the financial services have attracted particular attention. On the one hand, theoretical analysis and empirical research have addressed the dependence of financial services organizations — and/or the social regulatory arrangements and institutions that underpin them — on the establishment and sustenance of a climate of public trust (e.g. Morgan and Knights 1997; Dodd 1994). Here the issue is one of public confidence in financial institutions and their representatives.\textsuperscript{6}

With the relative decline of ‘welfare states’ over the last two decades, insurance companies, banks, building societies, and so on, have become dominant vehicles for advancing the economic security of populations (Knights and Vurdubakis 1993). On the other hand, researchers have investigated what we might call the construction of the ‘trustworthy customer’ through practices such as credit rating (Leysbon and Thrift 1998; Shaoul 1992), demographic analysis or direct marketing (Knights and Odih 1999). However, as Sundbo (1997: 123) has argued, financial institutions command considerable trust in western democracies, not least because of the perception that they have a quasi-public status in regulating the economy. In the present context, financial institutions constitute — to use Bourdieu’s (1971) term — the obligatory passage points through which almost all traffic in the virtual marketplace (e.g. e-payments, credit and debit transactions) have to pass.

Further ‘virtualization’ of organizations is expected to gather pace in the 21st. century as the Internet, through the medium of digital TV, becomes as commonly used a network as the telephone. That said, pundits and commentators anticipate the future development of virtual organization, but cannot yet point to many examples of its adoption or advanced usage. However, financial services is one area of economic life where ‘virtualization’ is encountered less in terms of futurological speculations and more in terms of concrete practical accomplishments. Financial services involve the manipulation of symbols rather than material artefacts. They are in effect the pre-eminent purveyors of ‘virtual’ goods. In the words of Negroponte (1995), it is a business of bits not atoms. Given that it is so information-based (Essinger 1996), it is no coincidence that this industry is at the forefront of experimentation with forms of virtual retailing. Virtual forms of distribution of financial services to a mass retail market are now well estab-
lished and extensive, as many of the established barriers to entry and sources of competitive advantage no longer necessarily prevail.\(^7\)

To date, one of the fastest growing\(^8\) virtual types of distribution in the United Kingdom has been telephone banking and insurance (e.g. First Direct, Direct Line). While the record of achievement of the new networks is, at least so far, mixed, in several European countries as well as in the United States, online banking is fast becoming more common. In California, for example, Wells Fargo bank reported to us that 1000 customers were signing up per day ever since its launch of Internet banking in May 1995.

Financial services companies can be seen to be caught in a dilemma. On the one hand, they are interested in improving their profitability through the construction of networks of remote distribution in the name of improved customer service and convenience, which can yield a cost or competitive advantage and therefore make a sustained contribution to bottom-line performance. Balanced against this, however, is the risk\(^9\) (or at least the perception of) fraudulent transactions, as well as customer resistance to the new, ‘virtual’ distribution channels (Knights and Odih 1996) fuelled by such perceptions of insecurity (MORI 1998; Kelley 1998). What difference does a ‘virtual’ environment make to the way the issue of trust is posed? For some, trust constitutes the Achilles heel of the virtual realm. Fukuyama (1995), for instance, lampoons the claim by an executive ‘from a leading-edge American networking company’ that ‘what is great about the Internet ... is that the actual business at the other end may be just a high school kid in his bedroom ... you wouldn’t know the difference’:

‘Damned if I would give my credit card number over the Internet to some high school kid. I don’t know much about the state of digital authentication, but I do know something about high school kids, and I wouldn’t trust them with taking out the garbage, much less with my valuable financial information.’ (ibid.)

Because of the ‘absence of trust’, Fukuyama argues, the virtual corporation is destined to ‘fall on its face’, but, of course the issue of trust in the virtual world is contested. Others have mounted a stout defense of the possibility of trust in cyberspace (e.g. Bennett 1996). The ‘cybereconomy’ it is claimed, ‘will be a high trust community’ (Davidson and Rees-Mogg 1997: 371). Moss-Kanter, for instance, contends that the shift to cyberspace — where organizations are less clearly (that is hierarchically) structured and more diffuse — need not entail loss of trust. Rather, the problems stem from the virtual organization’s residual cultural entanglement with its bureaucratic Other:

‘... many have not yet shifted their organizational style from the machine age to the mind age .... Instead of creating a new culture in tune with the expansive human possibilities of cyberspace, too many ... are confined in ‘bureauspace’ — the mechanistic culture of bureaucracy’ (Moss-Kanter 1995)

In other words, we should not yearn for the false security of a past mired in a culture of bureaucracy. Indeed, if cyber-enthusiasts are to be believed,
most compelling among these ‘expansive human possibilities’ of cyberspace is the ‘fluidity of identity’ that virtuality facilitates. On-line it is said that identity becomes the vehicle of role-play, of fluid and contingent self-expression:

‘You can have different identities in several different kinds of places. I am represented by a character known as Pollenator in Cyberion City and Funhead in WELLMUSE. When I use the “look” command to examine Sparks in Cyberion City, his identity description informs me of his resemblance to Thorin Oakenshield ... ’ (Rheingold 1995:154)

Alternatively, as the old Internet punchline would have it, ‘on the Internet, nobody knows you are a dog’. What is most relevant to our discussion is the Janus-faced representation of the ‘virtual realm’. For the converted, the most fascinating feature of ‘cyberspace’ is the implicit promise of ‘beating the meat’ by escaping the material limitations to identity or self-definition: ‘In cyberspace, there is no need to move about in a body like the one you possess in physical reality ... [which] will give way to a far more liberated notion of “body” as something quite disposable and, generally, quite limiting.’ (cited in Rheingold 1991: 191). In cyberspace then — Gibsons ‘consensual hallucination’ — participants can enter into creative relationships with one another in a manner said to be unrestricted and uncontaminated by the burdensome identifiers of race, gender, geographic origin, socio-economic contingency or physical appearance. All that matters is a capacity to participate competently in the ‘cyberlife’ of domains such as Cyberion City or LamdaMOO. This vision is closely paralleled in managerial discourse where it is anticipated that projects will bring together talented, competent cyberworkers, regardless of their social identity or location. Innovative virtual companies (like the school kid in his bedroom) will compete globally, purely within information networks, thereby obviating the costly provision of large offices, branch networks or standing armies of sales personnel (Martin 1996; Negroponte 1995; Woolley 1992).

At the same time, the faceless dealings in ‘cyberspace’ make it a congenial environment of deliberate dissimulation for fraudulent purposes. In the past, the impressive facades and marble halls of financial services companies played a crucial, if often satirized role, in reassuring clients about their security and trustworthiness. These traditional symbols are, it is claimed, rendered impotent when the interface with the customer is an ATM (Automated Teller Machine) or web site. When staring into cyberspace, the customer has no way of knowing whom she is entrusting with personal and financial information. Counterfeit web sites can be constructed just as criminals have in the past successfully created dummy ATMs (or attached devices to genuine ones) which have copied the cards and recorded the PINs of unsuspecting users. Bogus virtual companies can readily establish a presence on the Internet, only to vanish without trace (Dickson 1997; Houston 1997; Parkinson 1999). According to Mario Monti, EU Financial Services Commissioner, ‘faceless dealing over the Web could leave consumers at the mercy of criminals selling bogus products’ (Cumiskey 1998).
The reluctance of consumers to send money to strangers over new channels such as the Internet has prompted the argument that trust is increasingly conferred on the basis of reputation. From this perspective, the willingness of clients and customers to participate in virtual, remote forms of transaction is seen as depending upon a construction of trust engendered by the brand image of the trader (MORI 1998: cf. Lunt 1999). Attention to brand may then even override alternative strategies of competition. In which case, comparatively new entrants into the financial services market with a strong brand image and customer-base — such as Virgin, Marks and Spencer, General Motors and Tesco — may be able to penetrate the financial services market to an even greater degree than they have through more conventional distribution media. These companies have the further advantage of being unencumbered by the legacy of ‘pre-virtual’ distribution channels such as bank branch networks. Against this, it is worth noting that brand identity is not immune to technologically sophisticated jokers, info-terrorists and fraudsters (Lake 1998; Dickson 1997) Indeed, it is possible to use a brand name in constructing a counterfeit web site, a practice sometimes known as ‘site spoofing’.¹⁰

Even when fraudulent intent is absent, domain names constitute unreliable guides to identity and whatever trustworthiness this might confer. In two widely publicized cases, American journalist Joshua Quittner and MTV host Adam Curry registered with the Internet Network Information Service (InterNIC) the addresses Macdonalds.com and MTV.com, respectively, for themselves (Quittner 1994). As Davis (1994: 41) notes in his discussion of Vernor Vinge’s short story True Names, ‘cyberspace’s ultimate secret code is one’s True Name, one’s real human identity’. Remote distribution in which face to face contact or physical presence is devolved to the abstract domain of the network introduces a new level of uncertainty: identity. ‘Building [public] confidence in electronic commerce’, however, presupposes and requires ‘[confidence] about the identity of the person sending electronic messages … . The technology is available, but people need to be able to trust it and the companies supplying it’ (DTI 1999c). Resolution of the issue of ‘identity trust’ would thus overcome ‘one of the top-ranked barriers to the adoption of e-commerce today’ (Arthur D. Little & Co., cited in Identrus 1999).

(Micro)chips with Everything

As Norbert Elias (1939/1994) has argued, the civilizing process is synonymous with reducing the unpredictability of encounters with strangers. Historically, the (re)emergence of types of long distance financial exchange during the Middle Ages, promoted new forms of practice and discourse. Reliance upon an aristocratic code of honour with its hierarchy of interdependence, family connections, face-to-face encounters and ‘my word is my bond’ reassurances of trust were progressively supplanted by more impersonal mechanisms of exchange (Braudel 1981; Bouswma 1980). In the case
of banking and related activities, this was premised *inter alia* on the cre-
ation and circulation of written documents, orders, promissory notes and
bills of exchange dominated by the Italian banks (Spiegel 1991; Kerridge
1988). Through these media, spoken promises were rendered more stable,
mobile and combinable (Latour 1987; Bouswma 1980). This system
spanned across the urban centres of Western Europe and was regularly
employed by the Vatican in the conduct of its financial affairs (Spiegel
1991: 67–68). Trust was engendered through the use of instruments
intended to render the interaction between complete strangers, and over
long distances, more predictable.

Trust, it might be argued, becomes even more an issue in remote trading
where there is no longer the physical presence of parties or their repre-
sentatives to transactions.¹¹ There is increased fear of fraud and error when
the transaction is remote where ‘no cash changes hands’, to use a tellingly
physical metaphor. Electronic networks, are said to render the identity of
the transacting parties unstable: ‘That same “feature” that allows you to
disguise your identity in chat rooms also creates a serious ID problem for
e-stores (Waring 1999). Cyberspace thus even further exacerbates a range
of problems that afflict all ‘remote’ transactions, if only because of their
speed or ‘real-time’ character. The desire to create predictability and order
in electronic transactions has prompted many attempts to provide socio-
technical ‘solutions’ to a whole multitude of perceived problems of ‘dou-
ble contingency’ (Luhmann 1995). These include digital signatures (a
digital code unique to an individual or corporate user) used together with
public key encryption; SET (Secure Electronic Transactions) intended to
allow cardholder and retailer to authenticate each other; trusted third par-
ties; and so on. Here we concentrate on the role played by the ‘smart card’,
a plastic card that incorporates an integrated circuit chip, which is seen by
many as the most effective answer to these problems.¹²

‘Virtualization’ in the banking sector has been characterized as a move
from a ‘branch centric’ to a ‘card centric’ world. In place of face-to-face
transactions between bank tellsers and customers, the PIN used to access
ATMs has supplemented or displaced the signature as a means of personal
identification and access to services (Worthington 1998; Howcroft and
Beckett 1996; Howcroft 1993). The chip embedded in smart cards can hold
far more information than a magnetic strip and it can also carry out some
processing when in contact with a reading device. Its information-storing
and processing capacity means that a person’s identity can be more firmly
inscribed on the card than with a magnetic strip — for example, by embed-
ding digitized photographs, fingerprints, retinal or iris patterns. Smart cards
can also be plugged into a reader attached to a PC, a specially adapted tele-
phone, digital TV decoder, or digital GSM mobile phone, and used as a
more secure means of identification and/or to transmit payments electron-
ically and/or to download value. Basic memory-only disposable versions
are now in widespread use as telephone cards. A myriad of other applica-
tions is being developed or is in experimental use. For example, such appli-
cations are taking place in transport systems, the provision of health
insurance information and medical records, the identification of benefit claimants and distribution of benefits, the access to payment on digital networks, and as a substitute for cash in the form of an electronic purse, etc. Smart cards can check the right of any device to seek access to stored data as well as authenticating user identity.

As a result, smart cards have been championed as a highly effective means of reducing fraud and counterfeiting in financial and security applications. When used at the point of sale, cryptography embedded in the card reduces the need for costly and time-consuming on-line authorization. This makes its use particularly attractive in parts of the world where there is a limited telecommunications infrastructure. Perversely, it is the very existence of an advanced telecommunications system in the United States that constrains experimentation with more ‘foolproof’, yet initially costly, alternative systems of security.\(^{13}\) In principle, combining several different applications in a single card could massively reduce paperwork costs undertaken by banks, credit card companies or employers. Another constraint on this development is that it would require an unprecedented degree of co-operation between rival companies and disparate organizations.\(^{14}\)

The ‘do-anything, go-anywhere’ smart card offers a vision of a smoothly functioning, secure, and orderly world,\(^ {15}\) especially in countries where ‘law and order issues may be a problem’ (Worthington and Edwards 1998; Rigney 1998). In practice, the introduction of smart cards is far from orderly. Different organizations have produced a plethora of incompatible proprietary electronic purse systems, competing globally as well as within national boundaries. The introduction of smart card technologies has also given rise to concerns over intrusive surveillance, and new problems of disorder. Smart cards are viewed as opening up new opportunities for money laundering, fraud and the theft of identities (e.g. Kocher 1997). This feature of ‘virtuality’ is currently a source of concern among consumers, citizens and civil libertarians (6 and Briscoe 1996). They worry about the nature and privacy of information, commercial misuse of personal data, and even more about the vastly increased potential for government surveillance and control.

While our focus is on financial service applications, it is worth noting that the smart card is only one among a range of other possible vehicles for the integrated circuit chip. Notably, similar applications have been commended for the electronic tagging of offenders (Aungles and Cook 1994), juveniles under curfew, newborn babies in hospital wards, the senile and the mentally ill (Bloomfield 1998). All such applications constitute attempts to ‘bind time and space’ (Giddens 1990), or, as Bloomfield (1998: 1) puts it, they ensure the presence of the tagged individual ‘in the right place at the right time’ — and thus provide a technical ‘fix’ to a range of problems of social order. For example, recent UK Government proposals envisage the tagging of registered pedophiles so that the alarm will be raised every time they approach a school or playground (The Sunday Telegraph, 28/11/99: 2). The smart tag and card would then appear to be implicated in strategies of trust and distrust/control respectively. The consumer of financial services is the
carrier (but typically not the owner) of the card. S/he represents the category of normalcy in contrast to those who are physically attached to a microchip, such as criminals or the mentally ill (those who cannot be trusted) and are therefore subject to strategies of control. This renders deviants permanently subjected to remote control, monitoring and surveillance (see Figure 1). The use of information technology to enact and stabilize this division would seem to confirm much conventional theorizing on trust and power/control as opposing alternatives. On closer examination, a more ambiguous picture emerges and, as we see below, the electronic strategies for the remote control of deviants begin to merge with those for identifying legitimate users of electronic devices in making financial transactions.

Technologies of ‘Ontological Security’: The Customer’s Eye and the Minister’s Finger

The range of information kept on a smart card, and the range of uses to which it can be put are, in principle, extensive. At the same time, the appealing features of flexibility and universal access compound the risk of substantial loss in a way that prompts attention to issues of security. One key issue is how to be sure, or to trust, that the presenter of a card (when using an ATM or accessing a website, for instance) has a legitimate right to use it. Resolving this issue is conditional upon providing a solution to the problem of identity: Who is trying to use the card? As noted in our previous discussion of the use of this technology in the tagging of offenders, the newborn or the infirm, physical attachment in the form of an embedded tag offers one way of addressing this problem. It is hardly surprising however, that, to date, the preferred technical solution for financial transactions has been the PIN number. However, the security traditionally provided by the PIN is now viewed as inadequate. This is not least because of their proliferation, for this compounds the limitations associated with the vagaries of human memory as users experience difficulty in remembering the PIN number for each card they carry. Of greater concern, PINs can be evaded. Most credit and debit card transactions in the United Kingdom do not require the use of a PIN. PINs can also be illicitly obtained by fraudsters (e.g. by attaching copiers to ATMs), misused by children, or willfully abused by disgruntled ex-lovers or anyone who gains access to the number.

<table>
<thead>
<tr>
<th>Type of user</th>
<th>Control</th>
<th>Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated circuit chip</td>
<td>Criminal deviant or infirm</td>
<td>‘Normal’ citizen</td>
</tr>
<tr>
<td>Chip</td>
<td>As tag</td>
<td>Card</td>
</tr>
<tr>
<td>Monitoring of</td>
<td>Attached</td>
<td>Voluntarily carried</td>
</tr>
<tr>
<td></td>
<td>Movement</td>
<td>Consumption</td>
</tr>
</tbody>
</table>

Figure 1
Trust and the Microship
One response to pressures to find a more effective means of manufacturing trust has been to collect and check details of users’ physical characteristics through the use of retina scans, hand geometry, fingerprints, voice recognition, digitized photographs, and DNA. For example, as digital cameras improve and become cheaper and an essential peripheral, retina scans may become a routine security check. The use of these and other such biometric identifiers shifts the focus in security arrangements away from terminal devices to the user. Biometric identifiers make security more portable (Maes 1998) as well promising to reduce the risk of fraud by making the appropriation or counterfeiting of personal identity supposedly impossible. An example of the practical use of a biometric identifier is in the design of red boxes used by Ministers in the British government. As a check against misuse, these now incorporate the authorized user’s fingerprint, via a sensor. The sensor is also sensitive to body temperature in order to ensure that the minister’s finger has not been severed. Smart cards with encoded fingerprint checks are already in use by Russian banks and certain South African companies (6 and Briscoe 1996: 29–30).

The first iris recognition trial in a UK financial services company is, at the time of writing, underway at the Nationwide Building Society, using a machine developed by NCR Financial Systems Ltd. A magnifying camera photographs the iris and the picture — converted into a barcode — is then compared with a database of customers’ iris patterns to identify the particular individual attempting to use the card. It thereby dispenses with the need for a PIN. The attraction of this particular method of biometric identification to this company was that, compared with other metrics, such as fingerprints, there is a low level of false readings and rejects. It was also believed that, if the price comes down, iris recognition would ‘offer a good way of signing on to PCs, signing on to mobile phones, starting cars, whatever’ (Nationwide, Head of Business Futures). This same technology is already in use in the US prison system as a means of establishing the identity of the prisoners being released:

“We chose iris recognition technology over other biometrics because we want to be absolutely certain that we are letting the right person walk out of the door ... . Stealing or counterfeiting another person’s identity will prove unsuccessful.’ (Cpt. J. Fontana, Sarasota County Detention Centre, cited in promotional material by IrisScan Inc. at www.iriscan.com; see also Bloomfield 1998)

For Nationwide, the test is as much about gauging public reaction as it is about assessing its technical effectiveness as a replacement for PIN numbers. Will it contribute to the process of manufacturing trust by offering (commercially) valuable reassurances about the security of new, virtual distribution systems? Alternatively, will it arouse suspicion and hostility as criticism is leveled against the intrusiveness of such devices?

“It was just to see what is the value of providing a biometric instead of a PIN? What is the reaction of the press going to be? What is the reaction of the customer going to be in the sense that you know as soon as you start talking about it. In a more abstract, a more academic sort of way, you start hearing, well, there is going
to be a big backlash because of the civil liberties issue, and things like that, and there was only one way of finding out about it and let’s try it, [see] what is the real reaction going to be to this sort of stuff ... ’ (Nationwide, Head of Business Futures)

(Another pilot, of a call centre biometric system — provided by Vocalis — which identifies the voiceprint of a caller was conducted in September 1999 (see also Cross 1999: 12).

Biometrics appears to offer a ‘fix’ for perceived risks and the resulting customer reluctance associated with ‘virtual’ transactions. Speaking on behalf of an initiative headed by Microsoft, Bull, Gemplus, IBM, Slumberger, SNI, Sun, Toshiba and Verifone aim to promote card-enabled PCs. Phillipe Maes (1998) defined security levels in the following terms: low-level security is enabled by ‘something you know: password’ whereas medium-level security is provided by ‘something you know + something you have’, such as a smart card + password. Finally, high-level security is achieved by a combination of ‘something you have + something you are’; namely a ‘smart card + biometrics’ (see Figure 2).

The electronic persona(e) whose liberation from the constraints of biography and biology had been celebrated by computer enthusiasts and Internet utopians (see earlier), is returned, via biometrics, to its bodily container. Biology constitutes Vigen’s ‘real name’ which the virtual realm had rendered unstable and elusive. The combination of smart card + biometrics is therefore potentially productive of the reinstatement of identity by anchoring it in a physical characteristic. To paraphrase Giddens’ (1990, 1992) argument on modernity, it is a technology of ontological security. That is to say, it is a means of ensuring ‘the continuity of things and persons’ (1990: 97), of rendering an absent Other stable and predictable.

At the same time, the power of this technology depends on overcoming any public suspicion of smart card technologies and the companies and institutions seeking to benefit from their implementation (6 and Briscoe 1996; MORI 1998). Issuer promoted biometric cards may appear to many to be a vehicle of a panopticism in which, ironically, the eye becomes the object rather than the agent of surveillance. On the other hand, these technologies have been defended as responsive to civil libertarian concerns, because smart cards and biometric identification may equally be welcomed ‘as a tool for security and anonymity’ (6 and Briscoe 1996: 530 that are much less intrusive and more reliable than established practices of examination and record keeping. As NCR, the manufacturers of the Nationwide system put it: ‘the question of consumer acceptance of biometric technologies at (public and private) end-points is still largely unanswered. To date, limited investigations have, not surprisingly, indicated a great variety of consumer concerns with this technology’ (NCR 1997). The trial of the prototype was in this sense a way of exploring this ambivalence, rather than simply testing the accuracy, power and robustness of the technology.

It is apparent from what has been said so far that the smart card is envisaged, by both managerialists and libertarians, as a sort of obligatory pas-
Figure 2. Security Levels — From Identification to Identify
sage point for all access to ‘virtual’ facilities: bank accounts, health information, access to buildings, use of a diverse range of services, etc. It constitutes, in other words, a kind of universal interface, a tool of (cyber)administration. The smart card is, as noted at the outset, but one among a range of possible vehicles for the ‘attachment’ of the microchip to the person. ‘How far in the future will credit cards be worn rather than carried, and how long before every creditworthy shopper has a chip implant?’ asks the Financial Times, rhetorically (Money, 21–22/11/99: 1).

In fact, a survey on behalf of UK Neighbourhood Watch groups found that nearly 60 percent of respondents expected that microchips will be implanted into criminals so that their movements can be tracked (MMN, 19/11/99: 3). Clearly, increasingly effective transmissions through radio signals suggest the possibility of alternative arrangements to the card, such as microchips carried in clothing or body jewellery and activated remotely.16

In one of its reports, the Institute of Chemical Engineers proposed that microchips could be sealed in biocompatible glass and implanted in the body, generating a constant stream of real time medical information to a health centre17 (Warwick 2000). This, then, may be seen as the next (and ultimate?) security level in the Maes (1998) chart above. The ever-closer attachment of smart card to the body culminates in fusion, a cyborg.

The proposal in the report was enacted by a professor at Reading University, who had a microchip implant which enables his movements to be traced and access to be gained around the campus. Other suggested applications for the technology range from ensuring honesty at work and financial transactions (Uhlig 1998: 3) to the exchange of tender messages between similarly implanted lovers (Martin 1998: 49; Warwick 2000). The ambivalent status of the smart card as enhancing both autonomy and control has been graphically demonstrated by Brazilian artist, Eduardo Kac who, in the context of an Internet performance, had a microchip implanted in his ankle.

On one hand, the voluntary nature of Kac’s implantation can be interpreted as an act of trust in modern technology and its institutions. The backdrop of photographs of the author’s family displayed on the walls and visible during the webcast could thus be interpreted as an allusion to the increasing role of electronic media in the preservation of memory and the communication of social identity. At the same time, it is a manifestation of distrust: most of the artist’s family perished in Poland during the Holocaust. The location of the implant alludes to prisoner tags and slave chains. This kind of performance can be interpreted as a dramatization of contemporary trust/distrust in the (dis)ordering potential of microchip-based technology. It also articulates the ambivalent status, which the human/microchip hybrid occupies in (late/post) modernity: between subject and object, trust and distrust, autonomy and control, order and disorder.
Concluding Remarks

In Book II of Plato’s Republic, Glaucce narrates the mythological story of Gyges who accidentally discovers a ring, which can make him invisible. Gyges uses the ring to betray the trust of the Lydian king Candaules, seduce the queen, murder him and usurp the throne. The challenge which Glaucce presents to Socrates, is to show how trust could survive in a world in which such rings existed. Glaucce’s gedankenexperiment, in which the distinction between the just and the unjust is subverted and social order usurped by confusion and indeterminacy (Plato[Lee] 1987: 46–53), is of course not unlike Luhmann’s (1979) own counterfactual world. If the accounts of cyberspace and its consequences circulated by cyber-utopians and cyber-dystopians alike are to be taken seriously, society is currently grappling with a similar problem of order. The claimed consequences of the divorce facilitated by new electronic technologies between the physical and virtual worlds are, as we have seen, closely reminiscent of the ring of Gyges.

Commercial discourses of ‘virtuality’ have typically construed the ‘problem’ of identity as one of dis-association. Cyberspace, according to this view, makes possible the detachment of ‘virtual’ from physical identity, signifier from signified, thus creating an environment that is characterized by freedom and opportunity or alternatively by instability and disorder — depending on which guru you want to believe. What everyone agrees on, however, is the high level of uncertainty that characterizes the ‘virtual domain’. As commonly conceived, trust and control through power, have been seen as functionally equivalent strategies for absorbing uncertainty and dealing with the freedom and indeterminacy of other agents. However, ambivalence and indeterminacy continually usurp public discourse on, and engagement with, ‘smart technologies’ in ways that disrupt classification in terms of the trust vs control polarity. In the ‘virtual era’, trust in financial institutions depends upon trust in the technological systems they use, and, at the same time, trust in these technologies depends upon trust in the institutions which operate them.

This places the smart card — the proposed technological solution to Glaucce’s problem — at the centre of a number of ‘paradoxes’ typical of ‘information society’. The consuming public may express mistrust in the data collection activities of business in general, and financial institutions in particular (e.g. 6 and Briscoe 1996: 54–60). Yet, at the same time, it shows a willingness to ‘entrust’ ever increasing amounts of personal data to those same businesses and institutions in exchange for various benefits (The Economist 1/5/99). For instance, lack of public confidence in what supermarket chains (MORI 1998) are up to, goes hand in hand with divulging more and more personal information for what would appear to be the comparatively trivial benefits of loyalty cards (currently held by about 62 percent of British consumers [ibid.]). The vocabulary of (mis)trust appears to be at odds with behaviour, in a way similar to the examples given by Fox (1974: 66–67). Contemporary ‘card culture’ thus appears to be hopelessly mired in ambiguity, and indeterminacy. With echoes of
Foucault (1979), financial institutions (the symbols of trust) and prisons (the very embodiments of mistrust and control) may come to rely upon similar technological apparatuses. The power versus trust opposition has arguably often been productive in organizational theory. At the same time, our discussion points towards what we might call a symbiotic relationship between the two. Trust and (power assisted) control like all binary oppositions manifests, as Derrida (1981) argues, a continuous traffic within the two terms. In defining one another, the two opposites inhabit each other: they are caught in an ongoing undecidable exchange of attributes (Cooper 1986). In this paper, we have suggested the example of biometrics to illustrate this argument. Biometrically authenticated smart cards, of which financial services are expected to be important users, are to function as technological apparatuses for making an absent and invisible body present in the context of networks of remote electronic delivery. If the methods currently being tested by the Nationwide Building Society and other financial services organizations are widely adopted, the iris (or some other physical characteristic) of the customer will be scanned to confirm that legitimate use is being made of the card. Such methods of personal authentication constitute an uneasy mixture of strategies and activities, which elude unequivocal allocation along the trust/control opposition. For example, it is not far fetched to anticipate the extension of technologies of control, and their associated rituals of distrust, such as fingerprinting (the mark of the criminal suspect), to the whole population. This is in the expectation that, paradoxically enough, these technologies will contribute to manufacturing an atmosphere of trust in financial dealings.

**Notes**

* Funding support from grant number L132251046, the ESRC’s Virtual Society Programme is gratefully acknowledged.
1. By ‘virtual’, we mean forms of communication and transaction that are non-physical, at a distance, as opposed to paper-based and face-to-face.
2. "[Cyberspace may be seen] ... as a riot zone with the user not as orderly citizen but as digital looter" (Piper 1995: 234).
3. One hundred and ninety replies were received from regulators, financial services professionals, IT professionals and industry observers, including press, academics and consultants.
5. This is partly because the very medium of financial services — money — is based on a generalized trust in its acceptability and relative stability in exchange relations.
6. There have been a number of scandals in financial services in the UK recently, the worst of which was the mis-selling of personal pensions where consumers were given advice that was clearly at odds with their best interests. Recently, the Faculty and Institute of Actuaries have set up a panel to study ways of ‘significantly improving’ information and advice to consumers, in order to rebuild the credibility of the industry (Mitchell 2000: 1).
7. Examples of virtual channels of distribution include: electronic payments bank-to-bank (direct deposits and direct debits); use of credit, debit and ‘smart’ cards including electronic purses at point of sale; video-conferencing kiosks; telephone banking and financial services; online and Internet transactions, and interactive TV.
8. Another, of course, is the credit and debit card.
9. There are other risks that also revolve around the problems of trust. This is the risk and cost of proliferating new distribution channels, not as displacements of traditional high street
outlets, but as additional duplicate services. Low trust of the virtual outlets constrains the preferred strategy of displacement.

10. ‘The thieves create the impression that you are visiting one site while you’re really somewhere completely different. Even though you think you are shopping with a trusted brand, you are sending your information to a crank. If a spoofing site dupes a customer out of credit card information, it could be a costly con.’ (Lake 1998: 101)

11. As Weick (1987) notes: ‘face to face contact makes it easier to assess and build trust and trustworthiness … when those people are trusted and dealt with face-to-face, more information is conveyed, which should produce earlier detection of potential errors’ (p.117).

12. For instance, according to one of our respondents, a senior IT manager in a major banking organization: ‘I will shop, bank, whatever, using my Smart Card to prove that I am who I claim to be and all the clever [technical] stuff that goes on behind the scenes, all the encryption and certificates, I don’t see that. That will be in the Smart Card or in the PC. I don’t have to get my head around that, so we think things like SET which is the VISA-Mastercard, Secure Electronic Transactions, probably won’t have them, because it is too complicated and it relies on customers wanting to take an interest in stuff that they really don’t want to know about. Our research says that you as a customer, you just want us to tell you it’s OK and then you go shop, you don’t want all this fancy software stuff. So it is for us to put something really slick in there. I think it will all come into its own with Smart Cards in about two or three years time.’

13. As one of our research respondents in the United States pointed out, telecommunications in the United States are so efficient and cheap as to represent an obstacle to the costly introduction of new retail hardware to process more sophisticated smart card transactions.

14. As Steve Collins, of Barclaycard puts it: ‘There is no way the Barclaycard marketing people will let the Barclaycard details be stored on a Sainsbury Reward Card’ (FT Money, 21–22/11/99: 1)

15. According to Bennett (1996) ‘biometric validation such as voice print identification’ … makes possible the construction of orderly spaces …’ where people could carry out transactions with greater security and confidence than the general realm of cyberspace. Thus the twenty-first-century may see a return to a Victorian-like emphasis on trustworthiness and character in an environment no Victorian could have envisaged.

16. Intelligent Clothing in London, for instance has invested seven years in the design of a washable ‘intelligent vest’ capable of monitoring the state of asthmatics, head patients and pregnant women (Judd 1999: 20).

17. Such implants are under development by, among others, NASA and the University of California (Judd 1999).

References


Bourdieu, Pierre

Bouswma, William

Braudel, Fernand

Callon, Michel

Centre for the Study of Financial Innovation

Coleman, John S.

Cooper, Robert

Cumiskey, Annamarie

Cross, Michael

Dasgupta, Partha

Davis, Eric

Davidson, James, and William Rees-Mogg

Deleuze, Gilles

Deleuze, Gilles

Derrida, Jacques

Dickson, Ian
1997 Internet and financial services companies — of pirates and profit. Report for the Financial Services Forum, UMIST, Manchester.

DTI
1999a Promoting electronic commerce: Consultation on draft legislation and the Government’s response to the Trade and Industry Committee’s Report. Cm4417, DTI.

DTI

DTI

Dodd, Nigel

Drucker, Peter

Elias, Norbert

ESRC ‘Virtual society?’ Research programme ‘Memorandum to parliamentary research committee on E-commerce’, http://www.brunel.ac.uk/research/virtsoc/reports/ecom.htm
Essinger, James

Ezzamel, Mahmoud, and Hugh Willmott

Foucault, Michel

Fox, Alan

Friedman, Andrew

Fukuyama, Francis

Fukuyama, Francis

Gambetta, Diego

Gambetta, Diego, editor

Gibson, William

Giddens, Anthony

Giddens, Anthony

Hirst, Paul, and Jonathan Zeitlin

Hofstadter, Douglas

Hollis, Martin

Howcroft, Barry

Howcroft, Barry, and Anthony Beckett

Hutton, Will

Houstoun, Kevin

International Chamber of Commerce

Identrus

Judd, Alan

Kerridge, Eric

Kelley, Timothy
Knights, David, Fergus Murray, and Hugh Willmott

Knights, David, and Pamela Odih

Knights, David, and Pamela Odih

Knights, David, and Theo Vurdubakis
1993 ‘Calculations of risk: Towards an understanding of insurance as a moral and political technology’. *Accounting, Organisations and Society* 19/7–8: 729–764.

Kocher, Paul

Korzeniowsky, Paul

Kramer, R.M., and T.R. Tyler

Kyas, Othmar

Lane, Christel, and Reinhard Bachman

Lake, Matt

Latour, Bruno

Leadbeater, Charles

Lewicki, Roy, and Barbara Benedict Bunker

Lewis, D., and A. Weigert

Leyshon, Andrew, and Nigel Thrift

Lorenz, Edward H.

Luhmann, Niklas
1979 *Trust and power*. Cirencester: Wiley.

Luhmann, Niklas

Lunt, Peter

McGregor, Douglas

Maes, Philippe
Manchester Metro News

Martin, James
1996 CYBERCORP New York, AMACOM

Martin, M.
1998 ‘A chip that says “Darling I am thinking of you”’. The Mail on Sunday, 4 October: 49.

Mason, David, Gloria Lamshear, and Sally Coates

Misztal, Barbara

Mitchell, Jason

Morgan, Glenn, and David Knights, editors

MORI
1998 The lifestyle revolution. Slough: ICL.

Moss-Kanter, Rosabeth

NCR

Negroponte, Nicholas

Parkinson, Graham

Parsons, Talcott
1951 The social system. London: RKP.

Peters, Tom

Piper, Keith

Piore, Michael, and Charles Sabel

Plato

Quittner, Joshua
1994 ‘Writer has Ronald McDonald’s name as Internet E-mail address’. The Athens Daily News/Athens Banner-Herald, 16 October.

Raab, Charles

Rheingold, Howard

Rheingold, Howard

Richardson, G.

Rigney, M.

Ritzer, George

Sabel, Charles
<table>
<thead>
<tr>
<th>Sabel, Charles</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Sako, Mari</th>
</tr>
</thead>
<tbody>
<tr>
<td>1992 <em>Prices, quality and trust: Inter-firm relations in Britain and Japan</em>. Cambridge: Cambridge University Press.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sennett, Richard</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Shaoul, Michael</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Spiegel, Howard W.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Stanworth, Celia</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Sundbo, Jon</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Tsang, Linda</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Uhlig, Robert</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Wallich, Paul</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Waring, Becky</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Warwick, Kevin</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000 ‘Cyborg 1.0: Kevin Warwick outlines his plan to become one with his computer’. <em>Wired</em>, February: 144–151.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Weber, Max</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Weick, Karl</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Woolley, Barbara</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Woolgar, Steve</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Worthington, Steve</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Worthington, Steve, and Vic Edwards</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Zand, Donald</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Zucker, Lynne</th>
</tr>
</thead>
</table>