J. WORKPLACE RIGHTS, Vol. 13(2) 167-183, 2008

FORENSIC COMPUTING IN THE WORKPLACE: HEGEMONY, IDEOLOGY, AND THE PERFECT PANOPTICON?

BERND CARSTEN STAHL
De Montfort University, Leicester, United Kingdom

ABSTRACT

Forensic computing is an emerging academic discipline and professional field. Most publications in the area concentrate on technical issues related to the provision of digital evidence that can stand up to scrutiny in a court of law. There is a generally shared assumption that forensic computing activities are legitimate and in the best interests of society. This article aims to shed doubt on that prevailing narrative. The article uses some of the concepts of critical theory as applied in critical research in information systems and critical legal studies to point to some potential problems of forensic computing in the workplace. Drawing on traditional critical theory, the article argues that forensic computing can be used as a hegemonic means to uphold ideology even when it is used in law enforcement. Further problems arise due to the use of forensic computing by private organisations. An obvious use to which forensic computing can be put in corporations is that of employee surveillance. The parallel between forensic computing and the Panopticon is explored. The article concludes by discussing the relationship between the different critical approaches and the ways in which these approaches can inform us about the future use of forensic computing in the workplace.

Crime is ubiquitous, so are computers, and, consequently, so is computer crime. Computers and other information and communication technologies (ICTs) can be used as tools of conventional crime and they may lend themselves to qualitatively

doi: 10.2190/WR.13.2.e
http://baywood.com

new crime as well. We increasingly feel threatened, on an individual and social level, by criminal activities. These are committed by individual criminals, participants in organised crime, and terrorists. In order to address these threats, we need individuals who are capable of tracing electronic activities, securing technology, and supporting the prosecution of computer criminals. Such individuals are experts in the field of forensic computing (FC). FC is thus an important tool in the legal and legitimate fight against the dark forces who jeopardise our collective aims and individual good lives. Or is it?

The previous paragraph paints what may be a somewhat simplified picture of the public perception of FC. It probably represents the view of a considerable number of the students who sign on to study for FC degrees. This simplified view obscures legal disputes as well as social questions related to the emerging field and discipline of FC. Arguably, it does not do justice to the complexity of an academic discipline and a field of practice. Worse, it helps obscure specific interests that shape the field of FC and render natural and objective what is probably better described as the outcome of political and social struggles.

An added complication is that all of the above considerations refer to FC in law enforcement. A strong assumption that legitimises FC in this setting is that we live in a society whose institutions are reasonably well justified and that FC activities are strongly scrutinised by the legal system. The collection and presentation of evidence must be guided by legal guidelines and FC investigators have strong incentives to adhere to such rules, to ensure that their work will not be disregarded in a court of law. These assumptions change when FC activities no longer take place in law enforcement but in a private organisation. FC tools and techniques can then be used for different purposes, whose lawfulness is not always clear and whose ethical justification is even more questionable.

In this article, I develop a critical narrative concerning FC. I start by outlining the concept and social practice of FC, concentrating on the United Kingdom (UK). This provides the basis of a critical analysis that draws on classical critical theory as developed by the Frankfurt School but also on Foucault's writings, in particular his views on the Panopticon. The critical analysis leads to a consideration of possible means of addressing the downsides of the use of FC technologies in the workplace.

The purpose of the article is to raise doubts with regard to the usually unquestioned legitimacy of FC. The use of various ideas developed from various streams of critical theory is meant to facilitate a critical reflection on current practices and regulations. The article touches on many aspects of contemporary industrial and technological societies and will not be able to do justice to all of the discourses it relies on. However, in the spirit of much contemporary critical research, it aims to uncover overlooked viewpoints and thereby promote discourses that hold the potential to improve social practices.

CONCEPTUAL FOUNDATIONS: FORENSIC COMPUTING AND CRITICAL RESEARCH

This section introduces the concepts of FC and goes on to discuss the theoretical foundations used for the subsequent critical analysis.

Forensic Computing

Forensic computing is a developing field and therefore most of its central concepts are still very much in flux. In this article, I will use the term "forensic computing" (or FC), even though other terms, such as computer forensics or digital forensics or cybercrime forensics, are also used in the literature. There may be legitimate differences between these terms, but they are not sufficiently pronounced or widespread to necessitate conceptual distinctions.

A first approximation of a definition of the topic could be the one suggested by Wall and Paroff (2005: 1), who define FC as the "who, what, when, and how of electronic evidence." Its purpose is to reconstruct events, focusing on the computer-based conduct of individuals or groups. Put differently, FC is "the analysis of data processing equipment such as a computer, a network, and others to determine whether that equipment has been used for illegal or unauthorized purposes" (Mitrakas & Zaitch, 2006: 269). The generally accepted purpose of FC is to serve as a means of law enforcement. FC is the "analysis of computer data with a view to its presentation in a court of law as admissible evidence" (Mumford, 1999: 160). FC is an application of computing sciences to legal questions, in particular to detect, collect, and analyse evidence with a view to its admissibility in legal proceedings, in a manner that is equivalent to established forensic sciences such as odontology, structural engineering, pathology, serology, and so on (Wall & Paroff, 2005). FC "refers to the tools and techniques to recover, preserve, and examine data stored or transmitted in binary form" (Kenneally, 2002: 8). As the name suggests, FC is focused on the use of computers and the evidence their use can provide. However, it is difficult to distinguish between computers and other sorts of information and communication technology (ICT) due to the increasing convergence of different technologies. FC is thus often held to include questions of evidence in digital form in general, including evidence provided by the use of such devices as personal digital assistants (PDAs) or mobile phones (Myers & Rogers, 2004). This inclusion of different technologies leads to problems, as some technologies or aspects of them are well established (e.g., the collection of evidence from hard drives) whereas others pose new problems (e.g., the collection of evidence from networks that need to remain switched on for business purposes). Some authors consequently suggest distinguishing between computer and network forensics (Malinowski, 2006), and other such distinctions are imaginable. For the purposes of this article, such issues are secondary and I will thus continue to use the term "forensic computing."

In practice, FC practitioners work on all sorts of digital devices in order to find legally relevant evidence. The prime example of such activity is the investigation of charges of child pornography by an analysis of a suspect's computer files. There are, however, numerous other activities, such as the recovery of customer data from a drug dealer's mobile phone, the recording of date stamps of e-mail communications to provide (or question) a murder suspect's alibi, and the analysis of a stock broker's e-mail system in order to find evidence of insider trading. In addition to their use in such criminal cases, FC activities are increasingly important in civil cases as well. Examples of this might include the investigation of a former employee's log files in order to establish whether she downloaded customer data before going to work for a competitor or the analysis of Internet files to establish the financial status of partners in a divorce case. These few brief examples indicate that the practice of FC can touch on all of the aspects of life that are related to digital data processing, which in practice means almost all aspects of life.

Critical Approaches

Readers of the *Journal of Workplace Rights* are likely to have their own views on the meaning of the term "critical research." It is nevertheless worth exploring the meaning of the term as it is used in this article, because it shapes the overall narrative of the article. In addition, there are many different views of critical theory, which are not always compatible.

Very briefly, critical theory (or critical research) in this article stands for the attempt to emancipate human beings, to overcome oppression and alienation. Its roots can be traced back to antiquity (Harvey, 1990), but its main origins are in the era of industrialisation. The foundational texts of critical research involve Marx's critique of capitalism. Developments of Marxism, in particular the "Frankfurt School" of social research, have provided the most prominent representatives of critical thought. These range from the original members of the Frankfurt School, such as Adorno, Horkheimer, Marcuse, and others, to current members including Apel, Habermas, and Honneth. Other theoretical discourses are counted among the reference theories of critical scholarship. These include poststructuralism, postcolonialism, and postmodernism, to name just a few.

In this article, I will combine some of the concepts of the Frankfurt School with those developed by Michel Foucault. Foucault's work is associated with concepts such as bodily discipline, regimes of truth, and the question of discourses. The main aim of his research as he described it in *L'ordre du discours* (Foucault, 1971) is to investigate the mechanisms that contribute to the legitimacy of discourses. His main concern is not the truth of discursive contributions but the criteria according to which they are perceived as legitimate by other participants in discourses. Much of his work deals with this question in one way or another, whether it is in his discussion of bodily discipline (Foucault, 1975), in his

discussion of sexuality (Foucault, 1976), or in his discussion of other topics of interest to him, such as madness. Foucault's academic approach, that is, his use of genealogy, or the archaeology of knowledge, is tailored to the understanding of how certain contributions to discourses gain or lose acceptability. Foucault's work is of particular interest to critical scholars in the area of technology because of his reinterpretation of Bentham's Panopticon, as will be shown below.

This mix of specific theories can give rise to concern, and there has been extensive discussion of the compatibility of the two approaches, in particular between Habermas and Foucault (see Ashendon & Owen, 1999; Kelly, 1994). Elsewhere (Stahl, 2004), I have argued that it is appropriate to combine these theoretical perspectives because they allow the identification of different aspects of interest to critical scholars.

Critical theory has found applications in a wide range of fields of inquiry. The present article draws in particular on critical research in information systems (CRIS) (for an introduction, see Howcroft & Trauth, 2005; Stahl, 2008b) and critical legal studies (CLS) (for an introduction, see Fitzpatrick & Hunt, 1987; Kelman, 1987; or Mansell, Meteyard, & Thomson, 1999). For a more in-depth discussion of these two traditions, see Stahl (2007). Scholars in CRIS and CLS agree on their rejection of prevailing orthodoxy, whether it is positivist IS research in the case of CRIS or black letter law in the case of CLS. They consciously aim to break with tradition and deconstruct current practices in academia and beyond. At their core, both promote the idea of emancipation, despite the shared knowledge that it may be epistemologically impossible to find out what exactly emancipation is and whether it has been achieved. Much of the critical enterprise is driven by the intuitive belief that current liberal society is not perfect and, moreover, that its claims and realities are contradictory.

Criticalists of both streams of research are thus united in their desire to investigate and address issues and problems that have relevance for social change and the furthering of emancipation. Both give great emphasis to the importance of power in social relationships, whether it is promoted and encapsulated by technology or by legal processes. A central concern is that of inequality, its existence and justification.

THE SOCIAL AND LEGAL CONTEXT OF FORENSIC COMPUTING

FC is a social practice that has its own dynamics, interacts with many parts of society, and plays a role in how society views and uses technology. In this section, I lay the conceptual foundations for my subsequent critical analysis of FC. I first describe the social reality of FC and argue that most graduates will have to find employment outside of law enforcement. In a second step, I then discuss the difference between FC in law enforcement and FC in private organisations.

The Social Reality of FC Practice

As indicated earlier, the typical assumption is that FC practitioners or professionals will practice in law enforcement. While this may have been true for most individuals who currently call themselves FC professionals, it is certainly subject to change now. The social dynamics of the field will prevent the majority of graduates from entering employment in law enforcement. The example of the UK shows that employment in FC will have to move to the private sector. In the UK, there are currently slightly over 50 territorial police forces. Each of these now has a high technology crime unit, but these units tend to be small, consisting of only a few officers. In addition, there is the national high technology crime force, now integrated into the Serious Organised Crime Agency. Then there are FC specialists in other agencies such as special forces and intelligence forces. The total number of these is not published, but it seems plausible that the number is somewhere in the region of 200 to 500. At the same time, FC has become one of the more popular subjects in schools and departments of computing or computer sciences. Many such departments in the UK have started FC degrees in the last few years, and these have proven highly successful. In my own school, for example, the FC degree is now the most popular (out of about 20 undergraduate options), managing to attract over 60 first-year students and outpacing other areas of specialisation such as business information systems or computer games programming. Anecdotal evidence suggests that similar situations prevail in other institutions. Sheer numbers thus ensure that the majority of graduates currently studying FC will not be able to find direct employment in law enforcement.

Some of them may be able to work for law enforcement in different ways. The UK police are increasingly ready to employ non–police officers for specialist tasks and FC is one area where this may apply. In addition, there are growing numbers of private consultancies in the area of FC, many of them supporting law enforcement. The police are often unable to process their huge backlog of cases and they are increasingly outsourcing cases. But again, the number of individuals working in this type of environment will be limited. A majority of graduates will have to find employment elsewhere. The most likely place for them to find employment will be the IT departments of private organisations. FC graduates have a good understanding of ICT security, and they can thus work in security positions or in traditional computer scientist positions such as those of network administrator, webmaster, and so on.

FC in Law Enforcement and Private Organisations

There are substantial differences between working environments in law enforcement and in private practice. These have to do with the objectives of FC activities as well as the regulatory environment in which these activities are carried out.

One reason why we may perceive law enforcement activities as legitimate is that they are carried out in the judicial system, whose main aim is that of achieving justice. Justice is meant to be impartial. Perpetrators are caught and tried on the basis of their infringement of laws. Laws represent the population's view of what is right and wrong. Crimes are therefore punished, in a manner independent of the person and for the greater good of society. Clearly, such a view is naïve, and the critical legal studies movement has expended considerable effort on developing a more realistic description of the legal system. Poor people and people from minorities are more likely to be punished. Justice is not equal but prefers the ruling majority. The perception of crimes depends on the individual's characteristics.

Despite all this, the legitimacy of the legal system and law enforcement hinges on acceptance of the narrative of its being just and impartial. While this may be a fiction, it is a strong fiction and one that the public widely accepts. One clear indicator of this acceptance is the public outcry whenever a contravention is observed, for example, when a police officer or a judge accepts bribes or when political influence is brought to bear on the legal system to influence the outcomes of trials. An important aspect of the legitimacy of the legal system and law enforcement is that legal processes should not be influenced by profit motives. When a high tech crime officer investigates the online harassment of children or indecent images of them, we expect her not to be profit driven. And, arguably, this is true to a large degree. Law enforcement is not profit driven; this allows it to be impartial, and this, in turn, legitimises the fact that it has very powerful tools at its disposal. The same does not apply to the private sector, which by definition is partial and aims at the maximisation of profits. Such maximising behaviour may also be legitimate but it will rarely be impartial. Considerations of justice and equality do not enter into commercial considerations at the level of the individual agent.

A second fundamental difference between FC in law enforcement and FC in private companies has to do with the environment and with regulatory oversight. FC aims to find hidden information and therefore has the potential to violate privacy. A legal right to privacy was introduced to the UK in the Human Rights Act 1998 (HRA), which made the European Convention on Human Rights nationally applicable law. The aim of the act is, however, to protect citizens from the state. It is not meant to be directly applicable to private organisations. The practice of human rights law has shown that the HRA does have effects on commercial organisations, but these are less stringent than they would be for law enforcement agents, who are directly bound by the HRA. In addition to the HRA, the UK passed the Data Protection Act 1998 (DPA), the national manifestation of European Union (EU) directive 95/46/EC, which requires EU member states to institute the Organisation for Economic Co-operation and Development (OECD) fair information principles (Privacy Rights Clearinghouse, 2004). The DPA gives individuals the right to review and change the data on them that is held by any type of organisation, private or public.

A final, important piece of legislation pertaining to the collection of data on individuals is the Regulation of Investigatory Powers Act 2000 (RIPA). The RIPA states that it shall be an offence to intercept a communication transmission, even if it takes place on a private network. There are, however, exceptions (section 4), which render such interceptions lawful. In section 3(1), some reasons for interception are named. They include quality control, national security, and crime prevention and detection. In practice, this means that employers have a right to breach the privacy of employees' electronic communications if they can establish a business interest for doing so.

While this brief introduction to privacy rights gives the impression that there is far-reaching protection of privacy and personal data in the UK, a deeper look shows that this is not entirely true. Law enforcement is bound by all of the regulations and by additional procedural rules, such as the guidelines of the Association of Chief Police Officers (ACPO, n.d.). In addition, law enforcement investigations must be geared to transparency as they will have to stand up in a court of law. The same is not true for private organisations. As I have argued elsewhere, DPA and RIPA (Stahl, 2008a) reflect the view that privacy rights do not extend to employment situations. Business considerations often override privacy concerns. More importantly, investigations in private companies do not necessarily aim at being transparent. While they may result in legal proceedings, for example, in employment tribunals where stronger privacy rights, as laid down by the HRA, will be upheld, they will in most cases not be used for such activities.

The differences in motivation, regulation, and practice between law enforcement and commercial activity mean that FC can raise some additional concerns when applied in private companies. These concerns will be explored below.

CRITICAL VIEWS OF FC

Based on the understanding of FC, its definition and practice, and the critical approaches developed above, I now present a critical account of the field. In a first step, I take some of the traditional concepts of critical theory and argue that FC has the potential to contribute to problematic social developments. In the second step, I discuss more specifically the problems arising from FC when it is used as a means of installing measures for the surveillance of employees.

FC as Ideology and Hegemony

Traditional critical theory, by which I mean the Frankfurt School's branch of critical theory, is strongly based on Marx and a fundamental opposition to capitalism. The positions associated with it are frequently seen as academically problematic and politically no longer tenable. While such a view is understandable in the light of the political developments of the last 20 years, I believe that a lack of attention to critical theory's traditional concepts prevents us from giving attention

to some of the core concepts of traditional critical theory, which may be well suited to explain current social phenomena including FC. I therefore use this section to introduce some of the classical concepts, including ideology, hegemony, and reification, and apply them to FC.

Ideology in the critical tradition stands for widely shared but skewed perceptions of social realities. These relate to power, promote particular interests, and maintain one-sided and alienating relationships (Freeden, 2003; Hawkes, 2003; McLellan, 1995). That does not mean that ideologies are simply wrong. Ideologies cannot be wrong, in the sense that they form the basis of our understanding of reality. Indeed, they tend to be empirically supported (Gouldner, 1976). Ideologies are a main reason, however, for a lack of emancipation. An important question is how ideologies persist and are reproduced. Gramsci introduced the term "hegemony" to explain the mechanisms of "social psychological attempts to win people's consent to domination through cultural institutions" (Kincheloe & McLaren, 2005: 309). Hegemony in this article will be understood as the transmission mechanism that reproduces, legitimises, and perpetuates ideologies. Established power structures in organizations, for example, can serve as hegemonic mechanisms when they uphold one-sided and self-serving ideologies. Hegemony can use many different means to uphold ideologies. These include purpose rationality (i.e., a view of the world that considers means without questioning the ends), reification (i.e., the solidifying of social structures), and commodification (i.e., the turning of an entity into a tradable commodity), among many others.

The concepts of ideology, hegemony, and the different means of upholding ideology allow for a different view of FC from the one typically put forward by scholars and practitioners.

To some degree, the instrumental view of FC, which pervades much of the literature, has an ideological angle and is built on purposive rationality. FC is meant to create security or at least apprehend criminals. This leads to a hardening of what society perceives to be normal and abnormal and thus to a perpetuation of current, often arguably unjust practices (Poullet, 2004). Another means to hegemony in current FC discourses is that they further the invisibility of important issues that apparently play no role in these discourses. Questions of justice, crime and social status are often linked to race, class, and gender, for example. These issues are rarely, if ever, discussed in the FC literature, which tends to use an objective and positivist approach to reality. Gender is an obvious example of this rendering invisible of important issues (Adam, 2005). FC is often seen as part of computing, for which student numbers are highly skewed with men outnumbering women. Some of the most visible computer-related crimes, such as crimes relating to child pornography, are also offences committed predominantly by men. And yet the academic literature on FC does not consider gender an important issue.

Another form of ideology that is prevalent in FC is hidden in the populist and conservative background assumptions that accompany it. Many of the central

FC issues are capable of raising high emotional involvement, most notably child porn but also other issues such as hacking, viruses, or security (Nissenbaum, 2005). Clearly, all such issues are complex in their own right. However, in the FC field there is a tendency to simplify them unduly.

The ideological nature of the field is sustained by a number of interlinking means. A central one has to do with reification, with turning social constructions into "objective" things. Gender provides one example of this, where the "nature" of women becomes a piece of external nature, thus a thing, which is removed from scrutiny. Reification, commodification, and purposive rationality are linked to scholarly descriptions of the field, in particular the predominant positivist approach to research. Positivism is understood as a paradigm that is based on a realist ontology, an empiricist epistemology, and a correspondence theory of truth. This means positivists believe that reality exists independent of the observer, that objective observations can tell us the truth about reality, and that a statement is true if it corresponds with reality. There is much more to say about positivism, including a very different view of positivism that is held in legal studies, but suffice it to say that the brief characterisation given here provides an indication of some of the views that dominate FC and its reference disciplines, such as computer sciences, forensic sciences, information systems, and others.

An unconsidered acceptance of such contentious views is problematic in FC, for example with regard to the "reality" of digital evidence. A positivist will believe that digital evidence is out there and that, by following the right procedures, one can discover this truth and describe it objectively and unambiguously. Caloyannides (2006) points to one of the problems this can cause if judges and juries see digital data as inherently unalterable, when the opposite is the case.

Another problem related to reification is that of the prevailing view of technology. In a noncritical, usually positivist view of the world, technology is an unproblematic tool that can be used for desired purposes without further influence on these purposes. Furthermore, technology can be created for particular reasons, and it can be used to modify human behaviour in predictable ways. Such a view of technology is often called "technological determinism," and it has been widely criticised in the philosophy of technology. Technological determinism hides the social side of technology, which has been amply demonstrated by the research programmes of science and technology studies, the social shaping of technology, actor-network theory, and others. The danger for FC that arises from technological determinism is that a blind reliance on technological tools may lead to an inability to notice social structures, individual properties, exceptional circumstances, or other factors that should be considered. Again, the problem is by no means confined to FC, but given the immense influence FC can have on individuals who are subjected to its scrutiny, it stands to reason that such considerations should be of major importance in the profession, whereas, in fact, they are all but ignored.

The discussion of ideology and hegemony in FC was designed to show that the mainstream view of FC as intrinsically legitimate is at least questionable. This

is true for FC activities in law enforcement as well as anywhere else as long as the main assumption is that FC is used for the purpose of catching criminals and contributing to justice. However, as argued earlier, it is by no means clear that this is the only use of FC and the technologies it is based upon. The following section will therefore discuss an alternative scenario, namely, the use of FC for purposes of employee surveillance.

Forensic Computing as a Means of Employee Surveillance

The preceding section was built on the theoretical constructs that emerged from the Frankfurt School's tradition of critical theory. I now discuss the problem of employee surveillance, using Foucault's theories to argue that FC can be seen as an example of the Panopticon. The idea of the Panopticon was developed by Jeremy Bentham (1748-1832), who originally thought of it as a new design for prisons. The principle behind the Panopticon (from Greek: all-seeing) is that there is a central observer who can view all of the inmates without being seen himself. Bentham saw this design as beneficial because he believed that it would serve to resocialize criminals and make them productive members of society. Foucault developed this idea further, but viewed it in a much more sinister light. In *Surveiller et punir* (Foucault, 1975), he showed that surveillance is one means of ensuring compliance with the dominant social practices. The Panopticon as the perfect way of surveilling individuals not only ensures that people receive the punishments that society sees as fitting for their behaviour, but furthermore that they internalise the rules and sanctions and thereby develop the habit of self-surveillance.

Given the potential of information technology to collect data and to automatically process it, it is not surprising that many scholars interested in the social effects of ICT have built on this idea. Indeed, modern ICT allows a level of surveillance that far exceeds the simple methods of Bentham's Panopticon. The Panopticon is therefore a focal idea that links together work on privacy and technology. It is of particular interest to scholars who are interested in employee surveillance. The reason for this is that employee privacy and surveillance are much more contested than individual or data privacy that does not pertain to employment situations. The dominant view, at least in the Anglo-American world, is that individuals voluntarily enter into employment contracts and are therefore under an obligation to do during their working time as their employer demands (Nye, 2002). Employers have a corresponding right to check on their employees during work time or as long as employees are using their employers' property.

This line of reasoning is strongly contested (Weckert, 2005). One can argue that the power and information inequality between employer and employee is such that there cannot be a fair negotiation of contracts. In most cases, new employees will not be aware of surveillance practices when they enter into a

contract. A different issue has to do with the distinction between work and leisure. There are still many forms of work where such a distinction is unproblematic, but for most modern knowledge workers this is no longer the case. The temporal and spatial boundaries between work and private life vanish, leaving the surveillance of work performance perilously close to the surveillance of private activities. Furthermore, employers can claim a business interest in private activities such as gambling or alcohol or drug consumption, as these can affect work performance. The problem here is that there is some legitimacy to such claims and that individual and cultural perceptions of their limits diverge greatly.

The technologies and capabilities of FC have the potential to greatly influence organisational practices in this complex area. One important factor is the depth to which FC can go. Whereas in most traditional cases an infringement of company rules had to be observed in order to be punished, FC allows for detailed retrospective investigation of employee behaviour. The same technologies that can be used to trace Internet paedophiles can easily be used to check whether and when employees have used the Internet for non–work related purposes. In addition, such surveillance is completely covert. Whether someone's online activities are monitored and recorded is in most cases beyond that person's knowledge. Many organisations have acceptable use policies for their technologies and they often have reminders, for example, on log-on screens. It is unclear in most cases, however, whether these reminders are backed up by surveillance practice.

It is in particular this covert character of FC-enabled surveillance that renders it similar to the Panopticon. Modern decentralised work structures require employees to be self-motivated, and they make direct supervision by line management difficult. Other means of control have to be used, and a primary form of these is what Kohli and Kettinger (2004) call "concertive control." Concertive control is self-control by peer groups. Such control can be greatly enhanced and directed in the organisational interest by supporting it with Panopticon-like surveillance measures.

While the relationship between FC and employee surveillance is easy to establish, one should be careful to draw too simple a picture of it. As Foucault himself has consistently pointed out, there is no power without resistance, no control without negotiation. The idea that management can simply use FC as a means to enforce particular attitudes or behaviours is simplistic. In a classic study of the relationship between power and ICT, Bloomfield and Coombs (1992) have shown that a more complex approach to the relationship of power and ICT is required. Assuming that the use of FC for employee surveillance will have simple and predictable outcomes is an indicator of a belief in technological determinism, a belief that technology has objective and invariable properties that lead to determined outcomes: this has been discredited by social studies of technology (Grint & Woolgar, 1997).

A particular feature of the complexity of ICT and the power arising from the use of FC has to do with "anti-forensics" technologies (Casey, 2006; Harris, 2006). Such technologies are being developed in order to subvert digital forensic tools in order to avoid detection or prosecution (Newsham et al., 2007). Anti-forensics technologies can cause problems for law enforcement as they may cast doubt on the reliability of digital evidence. In the context of employee surveillance, such technologies open the possibility of counter-surveillance. The introduction of any technology leads to the introduction of vulnerabilities, and anti-forensics may prove to be one avenue to expose such vulnerabilities and subvert the process of surveillance.

Despite the caveats about the limits of FC as a means of surveillance and the problems of technological determinism, it is probably still fair to say that technology has certain affordances that make some uses more likely than others. Using this type of argument, one can easily make the case that FC has the potential to promote employee surveillance. As argued earlier, this is particularly problematic in commercial organisations because these do not undergo the same scrutiny or have to meet the same requirements of transparency as do law enforcement agencies. FC can thus become a means at the disposal of managers to be used to dominate employees and one-sidedly promote organisational goals to the detriment of legitimate employee needs, namely, privacy. One fact that can further this development is that private organisations are increasingly required by law to have FC capabilities. The existence of these capabilities can lead to function creep, in which investigative technologies and skills that were meant to protect the organisation from outsiders can be used against employees.

CONCLUSION

The purpose of this article is to cast doubt on the prevailing narrative concerning FC, which sees this activity as generally positive and legitimised. Using several strands of critical theory, including those of the Frankfurt School and the Foucauldian tradition, I have argued that a different view of FC is possible. It is important to recognize that these two strands of theory are closely interrelated. The underlying question has to do with the question of power and its legitimacy. FC, by its very definition, is meant to be intrusive. The question is: under what circumstances can such intrusion be justified? Justifications in the area of law enforcement are generally based on shared moral perceptions of the acceptability of particular behaviours. Highly visible instances of particularly revolting crimes such as those related to child pornography are generally used in order to project an aura of legitimacy around computing in law enforcement. I have argued that such a perception can be misleading, and that there are aspects of FC that can be better explained by the use of traditional critical concepts including ideology and hegemony. A different type of problem arises when FC is used outside of law enforcement and promotes particular interests. A predictable use of

such technologies in private organisations will be in employee surveillance. An added problem in this context is that the legitimacy of the power of management is more fundamentally contested than that of law enforcement officers. Surveillance as a resource for the execution of power (Introna, 2001) has the potential to increase managerial control and thereby change existing balances of power.

Despite the generally critical picture of FC that I draw in this article, the overall narrative should not be misunderstood as implying that I have fundamental misgivings about forensic computing. Every society requires rules, and these rules need to be enforced. In our current society, we generally agree that the rule of law is better than most alternatives. We therefore require mechanisms that allow the rule of law to be instituted in acceptable ways, and an important aspect of this is the provision of acceptable evidence. This is where FC finds its justification.

One of the contributions of this article is that it distinguishes clearly between law enforcement and private sector applications of FC. Both of these have legitimate applications, but they pose very different problems in terms of their legitimacy. Many of the issues raised here have an empirical component and require further empirical research. The cautionary tale I have developed here is based on plausible assumptions as to why an employer might employ a FC practitioner, but it is an open question whether these are borne out in organisational realities. It is beyond the scope of this article to investigate such issues further. Its purpose was to show that critical arguments can be made and that they are coherent and point to possible problems that FC should address in order to retain its ethical legitimacy.

Maybe a step back from immediate daily worries can help. Most social systems are created and maintained for some purpose. This purpose typically goes beyond narrow limits and follows some larger objective. In the end, the aim of institutions in modern democratic societies tends to be to facilitate the free and equitable existence of their citizens. Social institutions should be measured according to whether they contribute to this aim or not. Critical reasoning aims to question the underlying consensus and the things we take for granted, and to ask whether, on the basis of such a wider understanding, social constructs and institutions are desirable. If, by raising questions from a different perspective, critical research can contribute to the aim of creating a better and more just society, then it will arguably have fulfilled its self-professed goal of furthering individual and collective emancipation.

With regard to the private use of FC, questions related to the socioeconomic framework and to checks and balances need to be considered. FC offers powerful tools that can be used for a range of different purposes. It has the potential to seriously threaten privacy in ways that many of us are not aware of. Such uses may be legitimate in law enforcement but they may be less so in private organisations. The field of FC and society at large have not started to consider this distinction seriously. Part of the reason may be that there is limited general awareness of FC, and part may be that the field is moving so fast that it is difficult

to keep up with it. This should not stop us from thinking about how to address the challenges. There are a number of possible avenues to pursue. FC tools could, for example, be made available only to specific individuals in specific circumstances, in a fashion similar to the limitations on the use of certain chemicals or weapons in many countries. Another solution might be the establishment of professional bodies that could regulate the activities of FC practitioners and offer support in cases of conflict (Stahl, 2006). Maybe general legal regulations on privacy or intellectual property and other fields where conflicts of interest may occur will provide a way forward. This is again partly an empirical question, and it will be interesting to see whether the use of FC differs between jurisdictions with differing legislation on privacy. It stands to reason, for example, that the greater privacy protection afforded to European employees may lead to a use of FC and surveillance technologies that is different from the uses that are developing in the United States.

While legislation may appear to be the way forward, we should also remember that the critical approach, in particular the tradition of critical legal studies, cautions us about the use of legal remedies. Reliance on a legal system that has produced and upholds the capitalist structures of property and power to overcome these same structures is unlikely to be helpful. If FC causes a problem of surveillance, then the solution will not be found by regulating FC per se but by addressing the underlying problem in the relationship between employer and employee. This is not to say that a more stringent regulation of FC in private organisations is not desirable. It would seem to be perfectly reasonable, for example, for employers to be required to disclose any surveillance activities to the individuals they surveil. Such legal developments, however, would appear to be more an expression of a change in employment relationships than a cause of such a change. The entire problem discussed in this article, therefore, needs to be understood in its broader context. The core of the problem is not the technological performance of FC but rather the social relationships in which it is used and the question of the legitimacy of power in society. The present article can best be understood as a contribution to broader discourses, which need to be carried on in order to find generally acceptable solutions. What I hope I have done in this article is to raise awareness of the potential problems arising from FC. A more widely shared awareness of such problems is required to start the political and social process of finding specific ways of addressing them.

REFERENCES

ACPO. n.d. ***Good practice guide for computer based electronic evidence.*** Retrieved from www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf, May 2008.

Adam, A. 2005. ***Gender, ethics and information technology.*** Basingstoke, UK: Palgrave Macmillan.

Ashendon, S., & Owen, D. 1999. ***Foucault contra Habermas: Recasting the dialogue between genealogy and critical theory.*** London: Sage.

Bloomfield, B. P., & Coombs, R. 1992. Information technology, control, and power: The centralization and decentralization debate revisited. ***Journal of Management Studies,*** 29: 459–484.

Caloyannides, M. A. 2006. Digital "evidence" is often evidence of nothing. In P. Kanellis, E. Kiountouzis, N. Kolokotronis, & D. Martakos (Eds.), ***Digital crime and forensic science in cyberspace*****:** 334–339. Hershey, PA: Idea Group.

Casey, E. 2006. Investigating sophisticated security breaches. ***Communications of the ACM,*** 49(2): 48–54.

Fitzpatrick, P., & Hunt, A. 1987. ***Critical legal studies.*** Oxford: Blackwell.

Foucault, M. 1971. ***L'ordre du discours.*** Paris: Gallimard.

Foucault, M. 1975. ***Surveiller et punir: Naissance de la prison.*** Paris: Gallimard.

Foucault, M. 1976. ***Histoire de la sexualité I: La volonté de savoir.*** Paris: Gallimard.

Freeden, M. 2003. ***Ideology—A very short introduction.*** Oxford: Oxford University Press.

Gouldner, A. W. 1976. ***The dialectic of ideology and technology: The origins, grammar and future of ideology.*** London: Macmillan.

Grint, K., & Woolgar, S. 1997. ***The machine at work: Technology, work, and organization.*** Cambridge, UK: Blackwell.

Harris, R. 2006. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. ***Digital Investigation,*** 3: S44–S49.

Harvey, L. 1990. ***Critical social research.*** London: Unwin Hyman.

Hawkes, D. 2003. ***Ideology*** (2nd ed.). London: Routledge.

Howcroft, D., & Trauth, E. 2005. ***Handbook of critical information systems research: Theory and application.*** Cheltenham, UK: Edward Elgar.

Introna, L. 2001. Workplace surveillance, privacy, and distributive justice. In R. A. Spinello & H. T. Tavani (Eds.), ***Readings in cyberethics*****:** 418–429. Sudbury, MA: Jones and Bartlett.

Kelly, M. 1994. ***Critique and power: Recasting the Foucault/Habermas debate.*** Cambridge, MA: MIT Press.

Kelman, M. 1987. ***A guide to critical legal studies.*** Cambridge, MA: Harvard University Press.

Kenneally, E. 2002. Computer forensics: Beyond the buzzword. ***;login:,*** 27(4): 8–11.

Kincheloe, J. L., & McLaren, P. 2005. Rethinking critical theory and qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), ***The SAGE handbook of qualitative research*** (3rd ed.): 305–342. Thousand Oaks, CA: Sage.

Kohli, R., & Kettinger, W. J. 2004. Informating the clan: Controlling physicians' costs and outcomes. ***MIS Quarterly,*** 28(3): 363–394.

Malinowski, C. 2006. Training the cyber investigator. In P. Kanellis, E. Kiountouzis, N. Kolokotronis, & D. Martakos (Eds.), ***Digital crime and forensic science in cyberspace*****:** 311–333. Hershey. PA: Idea Group.

Mansell, W., Meteyard, B., & Thomson, A. 1999. ***A critical introduction to law*** (2nd ed.). London: Cavendish Publishing.

McLellan, D. 1995. ***Ideology*** (2nd ed.). Buckingham, UK: Open University Press.

Mitrakas, A., & Zaitch, D. 2006. In P. Kanellis, E. Kiountouzis, N. Kolokotronis, & D. Martakos (Eds.), ***Digital crime and forensic science in cyberspace*****:** 267–290. Hershey, PA: Idea Group.

Mumford, E. 1999. ***Dangerous decisions—Problem solving in tomorrow's world***. New York: Kluwer Academic/Plenum Publishing.

Myers, M., & Rogers, M. 2004. Computer forensics: The need for standardization and certification. ***International Journal of Digital Evidence,*** 3(2): 1–11.

Newsham, T., Palmer, C., Stamos, A., & Burns, J. 2007. ***Breaking forensics software: Weaknesses in critical evidence collection.*** Retrieved from www.isecpartners.com/files/iSEC-Breaking_Forensics_Software-Slides.BH2007.pdf, May 2007.

Nissenbaum, H. 2005. Where computer security meets national security. ***Ethics and Information Technology,*** 7(2): 61–73.

Nye, D. 2002. The "privacy in employment" critique: A consideration of some of the arguments for "ethical" HRM professional practice. ***Business Ethics: A European Review,*** 11(3): 224–232.

Poullet, Y. 2004. The fight against crime and/or the protection of privacy: A thorny debate! ***International Review of Law, Computers and Technology,*** 18(2): 251–273.

Privacy Rights Clearinghouse. 2004. ***A review of the fair information principles: The foundation of privacy public policy.*** Retrieved from www.privacyrights.org/ar/fairinfo.htm, January 2005.

Stahl, B. C. 2004. Whose discourse? A comparison of the Foucauldian and Habermasian concepts of discourse in critical IS research. ***Proceedings of the Tenth Americas Conference on Information Systems:*** 4329–4336.

Stahl, B. C. 2006. Is forensic computing a profession? Revisiting an old debate in a new field. ***Journal of Digital Forensics, Security and Law,*** 1(4): 49–66.

Stahl, B. C. 2007. ***Prolegomena to a critical investigation of forensic computing.*** Unpublished LLM thesis, De Montfort University, Leicester, UK.

Stahl, B. C. 2008a. The impact of the UK Human Rights Act 1998 on privacy protection in the workplace. In R. Subramanian (Ed.), ***Computer security, privacy, and politics: Current issues, challenges, and solutions:*** 55–68. Hershey, PA: Idea Group.

Stahl, B. C. 2008b. ***Information systems: Critical perspectives.*** London: Routledge.

Wall, C., & Paroff, J. 2005. Cracking the computer forensics mystery. ***The Computer and Internet Lawyer,*** 22(4): 1–6

Weckert, J. 2005. ***Electronic monitoring in the workplace: Controversies and solutions.*** Hershey, PA: Idea Group.

Direct reprint requests to:

Bernd Carsten Stahl
De Montfort University
Faculty of Technology
Centre for Computing and Social Responsibility
The Gateway, Leicester LE1 9BH, UK
e-mail: bstahl@dmu.ac.uk