Preface

The chapters contained within this text reflect the value of Systems Thinking in the design and development of Information Technology (IT). Its contents also reflect the growing range and number of contributions that the *International Journal of Information Technologies and the Systems Approach* (IJITSA) attracts. The chapters cover a diverse range of topics such as Software Engineering, Knowledge Management, Surveillance, and Privacy. Readers will forgive me, I hope, for the rather crude grouping of these fine papers. I have taken the position that this text is devoted to the use of Systems Ideas in the development of Information Technology in its variety of forms. Rather than repeat the editorials for each of the relevant editions, I have instead written an overview of the use of Systems Ideas within the context of particular applications published in IJITSA. To this end, I have divided the book into two sections. The first section is concerned with information provision and the second with security and privacy.

The text is composed of papers from the 2010 and 2011 editions of the IJITSA. In general terms, the first section deal with ways of attempting to overcome the difficulties of IT provision through the examination of current design methods and how they can be improved. In some instances, these papers show a distinct move from a technically-based approach to what might be called a soft approach. That is to say one that takes into account the social systems in which IT resides. For this reason, we briefly explore the difference between a computer system (or data processing system) and an Information System (IS). It is important to do so as we reflect the methods of design. The text then moves on to the chapters that address the benefits and the dangers of IT supported security systems. It is here where we consider if technological surveillance, ostensibly there to protect its citizens, might have unwanted effects upon individual privacy and freedom, but first we begin with information technology provision.

INFORMATION TECHNOLOGY PROVISION AND FAILURE?

There are few that would contest the assertion that information is the most important commodity we have. Moreover, it stands to reason that the way in which we design these systems will have a significant impact upon those who use them. Yet over the past decade, there is evidence that large information systems fail. The end-user, or client, is often unconsciously considered by the designer as a component of a data processing system, rather than viewing technology as a resource within a network of human communication. We find that the reductionist paradigm that underpins these design methods is often found to be lacking when confronted with modern information system requirements and the complex processing that characterises human decision-making. To ignore the customs and practices of the intended users is to invite trouble and will lead to failure. For example, a manager is reported as saying he had not seen
one successful project in 25 years, which he put down to politics and lack of alliances of the technical
competent. He continued by saying that “…the problem is not technical but dismal management and
shoddy methods” (Caulkin, 2004). Cross (2005) echoes this contention by pointing out that large and
complex projects cut across different agencies creating management difficulties. He points out that most
government projects start with the intention of using off-the-shelf software that inevitably ends up being
customised for the users. A recent report states that “A plan to create the world’s largest single civilian
computer system linking all parts of the National Health Service (in the UK) is to be abandoned by the
Government after running up billions of pounds in bills. Ministers are expected to announce next month
that they are scrapping a central part of the much-delayed and hugely controversial 10-year National
Programme for IT” (Wright, 2011).

Of course failures are not confined to the UK, as IT projects have a poor record throughout the world
(see Kraft and Steenkamp [2010] in this text, who make a similar point). In 2005, Cross reported that
70% of projects in the USA failed to meet their timetable or budget or come up to specification. OECD
reported only 28% of all IT projects in the US were successful in 2000 (OECD, 2001). The reports give
several reasons for this lack of success, including differences between public and private sector projects,
project size, project isolation, government interface with IT industries, market and technical dominance
of IT companies, modernity of equipment, and the extent to which government retains IT expertise. It is
clear from these reports that the failure is rarely of a technological nature but arises from a combination of
lack of clarity in objectives, poor management, naivety, and unrealistic expectations (Computing, 2003).

Failure, then, results from a mixture of things, and there is scant evidence of a failure of technology.
One conclusion that can be formed is that reported failure is the result of human error and not failure
of the technology. We should remind ourselves that any enterprise information technology is used as an
aid to decision taking and policy-making. Once installed and operating, the technology rarely fails, and
yet the Information System that it supports is often reported as failing. It was estimated that in 2004 IT
spending in the UK hit £23Billion (£12 B from public sector) and yet only 16% of British projects are
successful, and it is not much better in the USA, which is at 28-34% (OECD, 2001; Computing, 2004).

The likelihood of avoiding future failures is doubtful, as there is little to suggest much has been learnt
from the recent past, but what is an IS Failure? Because of the considerable investment in Information
Technology to improve business efficiency, it is not surprising that computing power and efficiency are
considered by many to be synonymous. Attempts to define IS failure often tend to focus on a failure
to the take up the technology and its associated software, but success and failure are not as easy as this
to measure as the take up of the technology may relate to the lack of consideration given to the needs
of the end user (e.g. Myers, 1994; Stowell, 2010). Fortune and Peters (2005) characterise IS failure as
a “…product of outputs which are considered to be undesirable by those involved.” They cite Vickers
(1981) who perhaps proves a richer and more experiential definition as “A human system fails if it does
not succeed in doing whatever it was designed to do; or if it succeeds but leaves everyone wishing it
had never tried.”

Clearly, a failure can be caused for a variety of quantifiable reasons such as being over budget, tech-
nology breakdown, and so on, but the implications of Vickers’s definition is that it is the impact upon
the users and intended consumers that causes the greatest problems. Whilst the specific cause of failure
differs with each information system, what they have in common is economic and social calamity. The
failure of a large public IS affects not just those who operate the IS or use it as a management tool, it also
frustrates the sponsors, the designers, those who managed the project and, increasingly, the general public.
There are numerous reports of IS failure (see Fortune & Peters, 2005), but the puzzle is why do they continue? Lyytinen and Robey (1999) suggested that many information systems departments appear unable or unwilling to adjust their practices even when they fail to produce beneficial results. It would seem that lessons about failure are not being learnt and research into design methods are not taken up. This is a situation that one commentator described as being “…like a computer virus, endlessly replicate the mistakes of the past” (Caulkin, 2004).

If we accept Caulkin’s premise that the problem is not technical, then the problem of failure does seem to lie outside the technology. The Dunleavy and Margettes (2004) report places great emphasis on the relationship between government and IT companies. They suggest the politics of Government operation and technical expertise as being key factors in success. These are all points of great importance, but they are focused on procurement of technology and not the failures following implementation. It is natural that as a digital processor is at the heart of most information systems it is often the acquisition and use of the technology that is cited as the success or otherwise of the Information System (Lynch & Gregor, 2004; Bisson, 2004). Many of the chapters in this text are concerned with this area (e.g. Conger, Software Development Life Cycles, and Methodologies).

INFORMATION SYSTEMS DESIGN

It is not uncommon for the methods of design adopted for information systems to be lacking in some respect. They are often methods whose origins are from the early days of computing where it was assumed that the computer would carry out the tasks that a human did not need to do, and the human activities would fit around the technology. Traditional Data Processing, as it was once called, is not concerned with information because it produces data that are used to guide routine activities without being explicitly interpreted to the activity. Human actors are informed by the data. That resulted in a profusion of data, which Ackoff (1978) referred to as an irrelevant abundance of data processing. With more powerful and easy to use technology, the modern day designer needs to take all aspects of the communication system into account, both human and technological.

We now recognise that although an information system, or system of information (Stowell, 2010), comprises a variety of technological devices, these are aids for human decision-making and not autonomous technical systems. They operate in the service of humans and not the other way around. Notwithstanding this, these significant failures in information systems continue (e.g. Wright, 2011). The prime reason for failure seems that IS development is undertaken as a technological project and not thought of as a system of information where, combined with the technology, it supports the system to be served (Wynter, et al., 1995). Because of this, there is a tendency to focus on the technology at the expense of engaging the end-user, or client, in the development and consequent ownership of the IS itself. This is not a new assertion, and similar observations could be found in the literature some decades ago, e.g. “An IS fails when it cannot fulfil the expectations and this incapability calls for stakeholder action” (Lyytinen, 1988). The difficulty has been, and still is, how the user, stakeholder, client, call it what you will, can engage in something as complex as IS development? IS development necessitates specialist knowledge of problem solving, technology, working practices, and some degree of clairvoyance.

When my colleague, Daune West, and I published our text (Client led Design, 1994), we were criticised because it was felt that non-technical clients did not have the skills to lead such a development
programme. Yet since that time, a significant number of researchers have attempted to find ways in which the client can have greater involvement and control over the project (e.g. Champion, 2001; Cooray, 2010; and chapters contained within this text). Our reasoning at the time, and still is, is that computers need to identify data objects, but people are interested in identifying and understanding what that object means. IS provision is about a total system of information, and as such, we need to consider the whole, that is all components, including human and technical.

Information Systems are formed from interrelated information units and relations between them. Our primary task then is to understand the purposeful actions of those that make up the system of interest and with the clients describe the information system that enables it. In other words, our first task is to consider the ‘system to be served’ and conceptualised in some way before the ‘serving system’ can be considered (Checkland & Scholes, 1990; Wynter, et al., 1995). Together with the clients, we can then envisage how the technology could be assimilated into their information system. It is only then that we are in a position to specify the technological support. It is what might be called a Voluntaristic theory of action (Parsons, 1949; in Burrell & Morgan, 2005, p. 84). This no trivial undertaking given the rate of change taking place within the global economy and the multi-relationships that the modern enterprise needs to maintain in order to survive.

OVERCOMING FAILURE?

The number of IS failures has prompted a variety of attempts to include the clients in development. In Software Engineering (SE), the more advanced approaches of IT development do show an awareness of the importance of user involvement. For example, the XP development cycle starts promisingly with “…end user stories that are used to estimate development time and define a plan for the release of applications… it makes it easier to get feedback from users as the whole application is developed” (Bisson, 2004). But the approach soon lapses into technology driven criteria for success as the satisfaction of the customer is measured by the delivery of software—“…satisfy them through early and continuous delivery of valuable software” (Agile Alliance Europe, 2004). Wautelet et al. (“Towards Knowledge Evolution in Software Engineering: An Epistemological Approach”), contained within this text, acknowledges that user requirements have been poorly taken into account partially because the modelling methods used have their origins in programming concepts rather than those more suited to human actors. They argue that Software Engineering “…is by nature a human activity… confront their visions of the software system they are building with users requirements.” They suggest a framework for SE based upon iterative development. In the special edition of IJITSA (Vol 4, no 1, 2011), Steencamp and Gonzalez explored the range of approaches related to Service Oriented Computing, in particular the use of a systems approach in the development process. These papers, which explore the use of IT to support collaboration and contribute to business transformation, are included within this text as distinct chapters. A variety of ideas are explored in this section that look at the ways in which easier integration between systems can be achieved as a means of providing a better foundation for adding new applications. Conger (“Software Development Life Cycles and Methodologies”) points to the fact that despite the number of research projects that have failed, SE still suffers from poor quality applications. She says that moving towards the development of usable applications embedded within organisational services requires some changes. Conger argues for more emphasis on usability, applications, testing, and improvements, and a shift to user involvement in design. The constantly changing nature of business and the need for the businesses’ IT
structure to follow suit is the topic in the paper by Karakostas and Zorgios (“Model Driven Engineering of Composite Service Oriented Application”). They propose a unifying framework in which workflow, data, and user interface are modelled. The ideas expressed in the special edition have some resonance with the Champion et al. (2005) paper in which the researchers explore the relationship between using soft ideas (e.g. SSM) and Object models to ‘navigate the gap’ between client requirements and technical support. The key consideration is how the users’ requirements can be successfully translated into an information system that meets their needs.

Despite the advances in software architecture and data mining, there is still a way to go before we can be confident of its value to IS provision. We find that the primary measurement of success is still in terms of working software. On the face, it is as good a measure as any, but we must ask ourselves is it good enough criteria for assessing the usefulness of an information system?

What seems to be overlooked are the intended clients who are best placed to define their Information System before we think about the data processing system part of the equation. IS development is usually technically biased because a computer system needs a concise specification and one that can be validated. The alternative of involving non-technically skilled clients in IS development is problematic. Aside from the time factors and costs involved, there is a certain level of technical understanding required. Attempts have been made by researchers to develop ways of involving the user, that is to say ways in which the end user, or clients, might take responsibility for the development of their information system.

The chapter by Kraft et al. (“A Holistic Approach for Understanding Project Management”) is an account of an investigation of the problem of IT project failure. These researchers also point out that the projects become problematic because of the mixture of technical, social, and economical endeavours. They use what they describe as a holistic approach in which Soft Systems Methodology (Checkland, 1999) plays and important part in the development of a conceptual tool, which they say will assist project leaders in recognising potential difficulties throughout the life of the project.

In the Hurster et al. chapter (“An Integrated Systems Approach for Early Warning and Risk Management”), they describe how they adopted an integrated approach in which the involvement of all related disciplines succeeded in providing a solution in the development of an early warning system for risk management. They involved all relevant stakeholders in their project as a means of meeting and defining their requirements, including the specification of communication links with the corresponding interfaces. These chapters (and others within) share a similar view that stresses the importance of engaging with the clients.

In his interview for IJITSA (Vol. 3, No. 2, 2010, pp. 57-63), Professor Silverman’s reply to the question about the future development of DSS has many similarities to the developments in Information Systems methods. Professor Silverman says that “…modelling social systems and societal dynamics is only possible by dragging onto the modelling stage, all of the exoteric information, and knowledge about the stake holders in a given social technical systems.” So there seems to be a general acceptance by SE and IS researchers and practitioners that modern IS provision is about enabling client participation. The consequence of this is a move towards methods that enable the client to take responsibility for the definition and consequent development of their IS as a whole, but how this is achieved is a more difficult proposition.
DEFINING INFORMATION SYSTEMS

IS design and development methods are predicated on satisfying a technical need because a computer and associated software needs a concise and verifiable specification. Given this situation, it is not unreasonable for the major actor in the design process to be a technical expert, and as a consequence, the design approaches employed are technically oriented. As we can see from many of the chapters contained in this text, several researchers, from Software Engineering and Information Systems, agree that we have to find ways of embracing the needs of the clients.

There is no doubt that attempting to define the IS without the full engagement of the clients can lead to difficulties during implementation and operation. Cooray (2010) undertook research in which she attempted to model the information systems requirements for a city library. Her approach, following Champion et al. (2005), Champion (2001), and Guo et al. (2000), used conceptual models used as part of SSM (Checkland, 1999) and AIM (Stowell & West, 1991; Stowell, 2012) as the basis for developing relationship models and class diagrams. These were quasi-technical models that she used to promote discussion with the clients as a precursor to the technical specification. Cooray’s work contributes to attempts to combine the soft aspects of IS provision with the technical elements in one unified approach.

However, client-centred approaches have been developed over the years, for example, Information System Engineering (e.g. Jackson Methodology, 1975), SSADM (1990), multi-view (Avison & Wood-Harper, 1986). Although these have improved the IT design, they have been less successful in providing a sound basis for Information Systems development. The continued level of IS failure suggests these ideas have had little impact. One problem is that the clients are not truly in control. This is because despite best efforts, these methods are still driven by technology and end up modifying the clients’ needs to satisfy the technical requirements. In their text, Client-Led Design, Stowell and West (1994) advocated IS provision be Client-Led rather than Client-Centred, but the difficulty here was in finding the method that moved the client from an everyday language definition of their information needs into a technical specification. Stowell and West used a conceptual model into a data flow diagram to achieve this, but this was only moderately successful, as it still meant a ‘leap’ from a non-technical to a technical description. Champion (2001) suggested an answer to this difficulty by suggesting that the client should ‘navigate’ from one to the other. This was developed further by Cooray (2010) in her research in IS provision in a city library, but one difficulty in involving the non-technical client and the technical expert is that one will see the information needs and one the technical potential. Following a less than satisfactory outcome to one publically funded project, the chairman of the public accounts committee stated, “One of the major problems was the ‘horrible interface’ between civil servants, who understand all there is to know about…. a system but know little of how a computer works, and technicians who just know the reverse.” He went on to say that, “…they don’t spend enough time at the start of the project explaining where they are both coming from” (Morris & Travis, 2001).

Because Systems is a meta-discipline, it can offer an alternative approach. In a paper printed in IJITSA in 2008 (Vol. 1, No. 1, pp. 25-36), we questioned if we were right in thinking in terms of information systems or if we should think more about systems of information. What we meant by this was that thinking in terms of Information Systems tends to place it in the same arena as information technology. Information Systems then become thought of as a physical artefact rather than in terms of the information that we need to make our way in the world. We ventured that we might be better thinking in terms of ‘systems of information’ that we need in order to function, whether it is in our daily private lives or in our working capacity.
By thinking about the systems of information we use, or need, we can separate those activities that are better undertaken by a human, such as activities that require tact and understanding, from those that are relatively routine, such as simple financial transactions. A system of information that encompasses the relationship between the computer, data processing, and human conversation into information and organization is proposed by Langefors (1995), called an integrated information system. Perhaps assimilation is a more appropriate description of the aim of the designer. The advantage of thinking how technology might be assimilated into the information system means that consideration of aspects of the wider system and issues such as decentralisation and IS strategy and activities that will influence the behaviour and form of an organisation are taken into account.

However if we accept this proposal, it follows that the methods we use to enquire into the systems of information are different than those that are primarily concerned with IT. An important distinction to be made is that the method of design should be client led not client centred. The client, rather than the technical expert, should take responsibility for the outcome of the design, but the difficulties of client involvement are many. For example, the association created by the form of the data may well affect interpreting the data. A sentence is conveyed to a third party who has the knowledge to receive it as a fact and no more. Information is more intimate and relies upon a shared understanding and synergy. We need to distinguish between facts obtained through interpretation and information obtained through inference drawn from conveyed factual knowledge. Langefors (1995) suggests that interpretation depends upon a clearly restricted set of knowledge whilst Inference involves a much more complex knowledge (and maybe these can be infinite).

**INTEGRATED SYSTEMS**

From a design point of view the IS professional is concerned with finding ways of defining that information system as a whole. The process can be broken crudely into the technical and non-technical requirements, bearing in mind that the former must be assimilated into the latter. Kljajic (“The Importance of Methodologies for Industrial and Scientific National Wealthy and Development”) reports attempts to combine methods and concludes that Simulation and a Systems approach (it is not clear which) should be fused with what is referred to as one holistic methodology. Like many who have gone before have discovered, attempting to combine methodologies has its own problems, e.g. conflicting epistemologies.

Langefors refers to the main task of the IS professional being concerned with the external properties of the IS, and the technical specialist, on the other hand, is concerned with the internal details. This separation of roles implies a division which is not compatible with assimilation; we would suggest that the solution is that the IS Professional acts as the navigator (Champion & Stowell, 2005), guiding the client from problem definition to satisfaction.

The process of modelling external details enables the client to say what they want their information system to be, leaving the navigator to describe how the information system is constructed. The notion of external properties as a means of describing the system of interest has some resonance with the black box notion in engineering and used as a modelling tool in Systems (Stowell & Welch, 2012). By considering, with the client, the output requirements of their notional system and then the inputs necessary to achieve them, the IS they want can go through a process of authentication (Champion & Stowell, 2002).

For Langefors, the idea of External Property definition is refined by describing two attributes, Functional and Interface. Functional, he suggests, is concerned with what the system will do for the clients and
users, and the way in which this is described is in everyday language. The Interface, on the other hand, has to do with how an object interacts with other objects and is of the technical kind and understood by software engineers. Importantly, there is a clear relationship between everyday description and specification, but the problem is how to do it whilst retaining client involvement. The papers in this section provide us with some interesting attempts to address these problems and much to stimulate our thoughts.

We now turn to the second section of the text, in which we have chapters relating to Security and privacy.

SECURITY AND PRIVACY

There are not many who would challenge the need to collect data relevant to matters of our security. Few would argue with the wish to have advanced warning of actions that might threaten our personal lives or the population. In modern times, we have found the need to increase security in order to protect us from those who wish to cause harm. To this end, there is an ongoing increase in security systems introduced to protect us from those who would ‘steal’ from us. Our increased use of technology to carry out transactions that hitherto would have been done through personal visits to shops and other businesses means that a new area of theft has opened up. Furnell et al. (“Prevention Actions for Enhancing Online Protection and Privacy”) draw our attention to our dependence upon on-line services and how our lives are dominated by email and mobile communications. Magkos (“Cryptographic Approaches for Privacy Preservation in Location-Based Services”) points out that just as the ‘system’ needs protecting against unauthorized access so too does the users’ data need protecting from unauthorized access.

These technologies have opened up new areas of crime, not the least, but perhaps the most disturbing, is that of identity theft. Many complain of the way in which our privacy is infringed through the way in which our use of the Internet is monitored and used as a tool for marketing, or worse. Professor Tsudik (“Interview with Gene Tsudik”) makes a valid point that many in our society have enthusiastically embraced a public forum for their personal feelings, such as blogs and social networks, yet complain of invasions of privacy. He goes on, “…increasing use of digitalization has led to some real concerns about privacy that weren’t there a decade ago. This includes medical and employment records….”

The growing dependence upon on-line communications has not been matched by citizens’ awareness of eSafety. Identity theft, financial losses, and failures to protect personal data have given rise to a growth in IT security. Although unwelcome, these systems of protection are seen as a necessary development by most private citizens, but have we got the balance right? The use of technology as an integral part of security is an area that the population has tacitly allowed to flourish (Katos, et al., 2007).

Alongside the increase in cyber crime, we are increasingly made aware of the rise of what is called cyber warfare. The Shorter Oxford Dictionary (2007) defines cyberwar as “…the use of computers to disrupt the activities of an enemy country, esp. the deliberate attacking of communication systems.” The attacks include official websites and networks, disruption or disabling of essential services, stealing or altering classified data, and crippling financial systems. The security firm McAfee surveyed 200 IT executives working for utility companies in 14 countries who reported Internet-based attacks on critical systems such as gas, power, and water. The report suggests that “… eight out of ten … networks had been targeted by hackers during the past year” (BBC News, 2011). In a separate report, the BBC news service reported, “Government networks receive around 20,000 malicious e-mails each month, around 1,000 of which are deliberately targeting them.” There are reports that the Defence firm Lockheed Martin,
which makes weapon systems that are sold around the world, was the latest to be hit. The same report announced the UK’s National Cyber Security Programme as part of the Strategic Defence and Security Review (BBC News, 2011).

Increasing surveillance also threatens individual privacy and the freedom of information (e.g. Daniels, 1994; Whittaker, 1999; Lyon, 2004; Stowell, 2007; Kwecka & Buchanan, 2011). It is difficult to keep a watchful eye over those things we wish to protect without an invasion of privacy. If we think about data collection, often undertaken in a crude and anonymous manner, it may be used in any one of a number of ways without our knowledge. As one security expert declared, “If you can’t find the needle, you have to take the haystack” (Harris, 2006). The increase in the use of technology in this way adds to individuals’ feelings of powerlessness and loss of privacy. For example, the monitoring of data collection points, e.g. CCTV and loyalty cards, are, to some degree, anonymous, but the individual has little, or no, idea how the data will be used. Daniels (1994) made the point that the change in bureaucratic systems of administration shifted control of surveillance from personal to the indirect. As a consequence, surveillance became depersonalised, making it more difficult to identify who is behind the surveillance.

Most citizens are unaware what personal data is held on them or how accurate it is. The State is in the position of observing its citizens, but we are unable to tell when we are being observed. In some respects, the use of technology in this way can be viewed as a new form of Bentham’s (1787) notion of the Panopticon or even in terms of a “superpanoptican” (Poster, 1989). In this case, technology replaces the physical prison but retains the key feature of observation of the subject who is unaware of being observed. Integrated networks mean that data can be collected about each individual in a variety of ways; some are explicit, some less so, with the potential of infringing on what most citizens consider to be their inalienable right to privacy; we need to protect the rights of the accused as well as the offended. Kwecka and Buchanan, in their chapter (“Minimising Collateral Damage: Privacy-Preserving Investigative Data Acquisition Platform”), consider the problems involved in protecting the privacy of all those involved in a cybercrime. They propose an approach that they suggest provides a balance between privacy of the alleged perpetrator and the victim.

**SURVEILLANCE AND POWER: TECHNOLOGY THE MODERN BOGEYMAN?**

To claim that technology is neutral is to ignore history. Technology can be used to monitor those who use it and how they use it. Access to the data that is available to us through the Web has both the potential to free and to enslave. ICT has the potential to enable citizens to gain a greater awareness of the society in which they live and improve life chances. It is now part of our culture, and it influences social behaviour and cannot be stopped. Kranzburg and Purcell (1967) reminded us that we have a responsibility here because although the process cannot be stopped “…nor the relationship ended … we must try to understand it and direct it to … goals worthy of mankind.”

In their paper (“Quis Custodiet Ipsos Custodies?”) Katos et al. (2007) question whether ICT’s are being used by Governments to control the population rather than protect it? They point out that information provides a significant source of power for those that have access to it, and the task of governing depends increasingly upon having access and the means of controlling information about individuals. The data might be collected with their knowledge, e.g. applying for a credit card or opening a bank account, or without their knowledge, e.g. CCTV images or the linking of apparently independent data such as loyalty cards and marketing data (Wilson, 2007). So we may ask, “Where does privacy of personal data
end and interference begin?” Foucault saw power as always being in the hands of a powerful minority, “... because they presented themselves as agencies of regulation, arbitration, and demarcation as a way of introducing order…” (Gutting, 1996, p. 100). We think that we would all agree that information is a source of power, and the way that it might be used is a means of exercising power. Giddens (1981, pp. 172) suggests that Foucault’s argument produced a “...too negative view of bourgeois freedom,” but the developments in technology coupled with fears of extremist actions have provided a reason for increased surveillance of the general population. We need to ask ourselves if there is a stage where there are too many measures of security, and does the collection and holding of personal data in whatever form exceed that required to make us secure?

Katos et al (2007) remind us of an important point, raised by Dandeker (1994), who said that the state cannot survive without a minimum line of consent, but legitimacy rests on the recognition that its acts are legal; and as such, it can adopt any policies that reflect that. It follows that legislation hurriedly brought following anti-social acts can lead to a threat to individual freedom. Indiscriminate and general collection of data under the policy of improving security also provides a means of ensuring that those with power exercise control over the population. Mavridis (“Deploying Privacy Improved RBAC in Web Information Systems”) points out that “Privacy awareness is increasing from the practice of modern organisations that utilize Web applications to collect, store, and process private information of users, usually gathered from monitoring their behaviours in order to provide more personalized and competitive services.” If business enterprises do it, one must assume the same applies to government agencies. As Dandeker (1994, p. 27) suggests, the control and surveillance of antisocial behaviour in all its forms provides an opportunity for policing and general surveillance of the population, and we suggest, unchecked, ‘Security’ becomes a new form of social control.

A document entitled “A Report on the Surveillance Society” (COM, 2006; Wood, 2006) indicates that, at times, a form of social segregation takes place without the knowledge of the citizen. For example, data obtained for individuals travelling by air is collected and analysed for reasons of security. Although this is understandable and few challenge its use, the way that it is used is undemocratic and the result of the way that ‘security’ is put into practice. It is likely most citizens, especially those travelling by air, are happy to accept such monitoring and control, but how much is too much? Privacy is about balancing individual needs with societal interests and a matter of self-protection, but, as Lyon (2004, pp. 193) continues, privacy is a privilege. This argument raises important issues about human rights and when and how we should decide that the monitoring and control of data affecting us all is sufficient?

Dean (1998) pointed out, “Government concerns the shaping of human conduct and acts on the governed as a locus of action and freedom. It therefore entails the possibility that the governed are to some extent capable of acting and thinking otherwise.” Katos et al. (2012) question if the checks made upon us nowadays are all necessary. They ask if they go beyond security. ICT provides a way of enclosing the population within what Dean refers to as “apparatuses of security” (Dean, 1998). The question we must ask is where does security finish and population control begin?

If we assume that the purpose of surveillance is to exercise control over a situation it monitors, e.g. crime reduction and terrorist activities, then we must take into consideration both the subject and the means of monitoring that subject. How much monitoring is too much? How do we know when we have gone beyond the use of technology for security into harnessing its use for social manipulation? Katos et al. (2012) put forward the argument for Ashby’s Law of Requisite Variety (LRV). LRV says that in any situation “…if a certain quality of disturbance is prevented by a regulator from reaching some essential variables then that regulator must be capable of exerting at least that quantity of selection” (Ashby,
1978, pp. 229). In other words, the variety in the controller must have as much variety as that which it seeks to control. In order to bring about effective control over any situation, the control mechanism must be capable of addressing as many different outcomes as it is possible for a situation to develop. In practical terms, this means the more complex the system the more difficult it is to predict its behaviour and the more difficult to exercise control. As a reminder of the practical difficulty, Sir David Pepper, the recently retired Director of GCHQ (the UK’s surveillance centre), said, “You would have to have so many people involved in the security services I am not sure what anybody else in the country would do” (Pepper, 2009).

**SUMMARY**

The majority of chapters in this text apply Systems ideas as a means of understanding a variety of problems within the general heading of IT. The many applications of the ideas provide examples of the way in which Systems Thinking is being used in Information System and Information Technology development. In this preface, we have attempted to add ideas to those contained within in the hope that it will encourage others to explore the use and appreciate the value of Systems Thinking and Practice.

We hope that you will enjoy reading this text.

*Frank Stowell*
*University of Portsmouth, UK*

**REFERENCES**


