We want security but we hate it. The Foundations of security technoeconomics in the social world. From Control to Surveillance*

Mauro Sandrini
msandrini@complessita.it
Teramo University, Italy

May 14, 2003

Abstract

The social aspects of security are becoming increasingly important, now that security is at the foundation of the upcoming Internet Operating System. We will not be able to investigate the human side of security issues without considering the other side of the coin: surveillance. Some 'Controlled Computing' proposals are emerging, which at times recall Orwellian scenarios; on the other hand the positive consequences that the surveillance stream inside society is producing, are rarely contemplated. By exploring the surveillance/control paradox we can achieve the 'Surveillance Computing' model proposal: a model in which the individual regains his or her data ownership in relationship with his or her community.
As a result, a new security concept will emerge that will express our security needs, and therefore will be more easily accepted by us, the people.

*This work benefited from the comments and contributions on the economics of evolutionary process by Dr. Ferdinando Cerbone, Ass. Coevoluzione - Reichian Studies Center, Bologna, Italy (www.coevoluzione.it).

1 The Internet Operating System at the root of 'New Society's Communications System'

[1] The Internet Operating System does not yet exist. But we are in the process of building it [23]. In the upcoming phase of this transition we will go toward a network operating system that will be a fundamental layer of human society's communications system.

The first signs of what is happening are already visible, thanks to tools like e-mail, joint productivity and social software, chat lines etc. As a result there is an enormous increase in the number of messages that each of us receives every day. It may seem as if we are evolving into *human message-processing machines* [24]. The designers' aim is to avoid this, leaving the mechanical work to automatic software systems [28]. The contradiction related to this approach is that we are fighting the environment's complexity by introducing technologies that increase the global system entropy. What we need, instead, are solutions capable of reducing this complexity.

Up to now, faith is what humanity has used to pursue this aim [15]:

> 'Faith reduces social complexity and therefore simplifies life by taking a risk'

Faith as an embedded value does not seem to belong to the emerging technological infrastructure. Security, on the other hand, is at the root of this developing network operating system. The aim is to build a world of 'trustworthy computing' [1] which will be part of a social environment, where the main value will be mistrust. The issue, then, is how will technology *embed* the social values [7]? Now the security concept core is entwined with that of fear. But fear of what?

Fear arises at several levels but we will concentrate on the two most important ones for our analysis:

The first level of fear concerns losing control of the profits obtained by the knowledge economy to date. Here the DRM (Digital Rights Management) becomes paradigmatic. Historically, copyright laws have worked rather well, to protect the owners of these rights[2] (who more often than not, are not the authors themselves [13]). However, the conflict arises when the contents start to reproduce themselves thanks to an evolutionary process based on the widespread possibility of sharing and communicating knowledge as never before. Here is where the copyright owners lose control and conflicts arise.

[1] To all intents and purposes the network operating system is going to build up an important layer of the 'society communications system', i.e. a system that we, as a society, are continuously producing. In this work, that is only the starting point of a wider one, we will refer to the 'technological structure' of this complex communication system and we will call it a 'network operating system'.

[2] Usually record companies, film studios and software houses. In fact the same representatives are the main promoters of the Trusted Computing Public Alliance consortium, now called the Trusted Computing Group consortium. For more details see Ross Anderson [1].

Open Source is the most well known case. Despite the fact that it is being taken into consideration in some business contexts (for example Oracle and IBM) it has just started to contaminate the old-new-economy. For example try to imagine what will happen if [5]:

> In early 2004, some bored geek starts an open-source OLAP [On Line Analytical Processing] initiative. Suddenly, Oracle doesn't think that Linux and its ilk are that cool any more
> *Gerald Boyd, Director of research,*
> *NCS Technologies Inc., Piscataway, N.J.*

This is exactly the fear that lies below the surface of the 'Controlled Computing' strategies and policies in its various forms and evolutions[3].

Trying to capture knowledge is like trying to capture air. You can lock it up but it will fly away as soon as the first crack appears. On the contrary, to be successful in locking up this knowledge will mean producing stale air that, in the end, will poison us.

When goods were made mostly of 'hardware' and contained small quantities of knowledge, the market barriers were made mainly of high investments in fixed assets and that was all. Now the competition borders are defined by the will of some 'bored geek' who wants to launch a new challenge. Therefore, the borders are completely different. But with the rising of 'Controlled Computing' this will definitely stop.

> The 'Controlled Computing' core issue is just this: the erection of economic entry barriers in the high intensity knowledge sectors through embedding software in the hardware.

The entry barriers will rise enormously as a result of the high capital investments that this innovation will require to newcomers. The fear is to lose control of a knowledge economy that is growing, and in the meantime it is sharing the value it is generating more and more.

The second level of fear concerns controlling the contents. There exists only one way to feed a knowledge economy: by sharing the knowledge itself in a learning social system [6] [19].

In the short term, an economy which controls knowledge to gain profits, may live with another, sharing based economic model[4]. This phenomenon may continue until the former model is able to extract profits from the latter. This is an important aspect of what is happening today with Open

[3]Henceforth we will refer to various denominations as well as to 'Trusted computing', 'Trustworthy computing' etc. for what they are in reality: 'Controlled Computing' as suggested by Ross Anderson in [1].

[4]For example see how the record companies have basically not registered falls in profits as a result of the net file sharing communities. See S. Lewis [14].

Source economics[5]. However, the process upon which this is based is non linear and evolving. It is in contrast with a linear based profit generation model which will become stable when market saturation arises (most of the time this is a monopolistic market when dealing with information goods). This stabilization may correspond to the opening of a new market, with the monopolist's death or with its complete transformation. If this occurs in too many markets at the same time this may mean the end of the global economic system.

On the other hand we have another evolutionary *Open* process that generates value through knowledge production, without the primary aim of pursuing a profit. This occurs, furthermore, without the markets' saturation but, on the contrary, without preventing the opening of new economic horizons. On one hand, the traditional market process reduces breathable air[6], on the other, it is possible to continuously discover new lands. Forces which are promoting the former economic model are based on mistrust and fear, the forces which feed the latter are curiosity, knowledge eagerness, desire for life[7]. The Open Source case is the most well known but the real interest of it lies in being paradigmatic of how knowledge can evolve and generate value. In a knowledge economy content is everything: software, music, video, books. Ever since DNA has been sequenced, even we ourselves have become 'itinerant code carriers'; in other words each of us is a content carrier. If the final aim of 'Controlled Computing' is content control then the richest content to take possession of is ourselves. Each of us for his or her genetic code[8].

Are we claiming that the Internet Operating System is not to be founded on security? No, what we are saying is that it must not be founded on the present security concept. It is this security concept that finds its true implementation on the 'Controlled Computing' trend. Another security model may emerge if we consider this as a true human and social need, instead of a gasping corporation system's last chance to avoid change [12]. Another way to face this idea of security/control may germinate only by embedding faith as a value in the network operating system. Perhaps the way to pursue this resides in the shadow line path that exists between surveillance and security without being dazzled by the preconceived ideas that these words very often trigger off.

We will now try to follow this path.

[5]There are several studies that aim at understanding Open Source economic process within the traditional economic framework [29]. In this way, as they assert, it is possible to explain *almost* all of what is happening. The reality indeed is that 'almost' in one complex evolutive phenomenon may become a big difference in the final result.

[6]This is evident in our economic situation that in recent times seems to have postponed the economic recovery until a near future that has not yet come.

[7]This is very similar to how scientific research was before it has been infested by patent's anxiety. The difference here lies in the fact that this pressure towards open knowledge comes from a wide social force instead of from an intellectual elite.

[8]Thanks to Dr. Ferdinando Cerbone for this contribution. Ass. Coevoluzione - Reichian Studies Centre, Bologna, Italy (www.coevoluzione.it).

2 Security and Society

Society's role in producing a security system has been underestimated in the past. This is not restricted to some social engineering techniques as it may seem from some media over exposure[9] but it emerges from a simple reality: attacks are based more and more on human system weakness instead of on technological weaknesses. If, as Ross Anderson says [1]:

> 'The complexity of the information flows within the real organizations tends to cause all the information to either float up to the highest level of classification, or float down to the lowest level'

then in today's organizations it is not possible to be positioned in the highest levels of classified information. This is why in a complex unstable economic environment, in which flexibility and adaptability are at the root of organizational behaviour [32], sharing knowledge is necessary. The highest levels of classification contradict flexibility and adaptability in a complex system. It is possible to compete only at certain levels of sharing or, that is, of faith. And faith, as we have already seen, brings with it some risks. This is why the lowest level of security is so widespread, and why it makes room for human based attacks. Today that security is becoming an important layer of the network operating system, and is no longer related to small organizationally closed entities, it becomes evident that security is a process and not a solution. A process, furthermore, that is strongly related to today's society evolution. Recognizing this may help us build safer systems, as they will become more closely related to how real organizations are.

With security technoeconomics we are laying the foundations of our actions and lives out there. Until we accept that we are looking for both security and surveillance in each of their community aspects we will fail in building a truly safe environment.

3 Surveillance at the supermarket: how consumers are producing control

Security and, the other side of the coin, surveillance, are inseparable. If security has to be at the centre of the network operating system it is impossible to consider it separately. Let us look at some facts concerning the ongoing phenomena [10][11]:

- 26 million surveillance video cameras have already been installed worldwide. Of these 11 million are in the United States;
- by 2006 the U.S. will prescribe that each cell phone can transmit the exact caller position during emergency calls. Obviously, this feature will become available on a mass basis for other localization aims;

[9] For example recently Kevin Mitnick, The art of deception [21].

- the top three U.S. automobile manufacturers will install in every vehicle an RFI system (Radio Frequency Identification system)[10];

- Telesurveillance now counts for less than 1% of the global surveillance phenomenon;

There are, furthermore, trends forecast on some new surveillance devices like the mounted-wall surveillance camera Nokia is going to introduce on the U.S. market by summer 2003. The cost will be under $500 and it will be capable of sending images to mobile devices. It is expected that the market value of such devices will be about 28 billion dollars in four years from now (Source: Wireless Data Research Group [8]). So there will be several dozens millions of items of personal video surveillance systems in a few years.

This is only the tip of the iceberg, the only visible one. The biggest part is hidden from the eyes of the common citizen: it is the weaving of the data which comes from the above systems, governmental and marketing databases. In spite of all the dependability related difficulties concerning the data collected [10] [11], it is possible to estimate that twenty years from now, in 2023, the equivalent of today's normal personal computer will suffice to monitor every single citizen, of the 330 million living in the United States at that time. In 2001 46.5% of companies were monitoring workers' emails and 36.1% were even monitoring organizations' computer files [10].

Are we facing a hyper tech version of Big Brother [18]? The answer to this question contains the security/surveillance paradox. Even if the process started with the big burocratic organizations (governmental and private) now it is the individuals and small organizations who are making it evolve in society.

If society *embeds* technology, then the technology we are producing today is embedding such values as fears and withdrawals, inside and amongst human beings. Such surveillance is not developing as in the Big Brother model, but rather it is something that emerges/happens every time we gain access to resources on the net.

Therefore, the collective emergent properties are generated starting from individual behavior, that then produces a dual relationship between the concepts of needs/rejection and security/surveillance.

In other words, our security needs take us toward a system that involves some special characteristics that most of us reject. This rejection produces some worrisome effects related to the global economic system's efficiency. For example individual productivity is reduced: in a working environment where the worker knows he or she is being monitored, the same worker is less open to sharing knowledge in a horizontal way. On the contrary, sharing is pursued by horizontal organizations and their knowledge management systems [11].

[10] An RFI is a small device which will be inserted into a product destined for the end consumer and that is capable, in the beginning, of optimizing the production process in transmitting to the producer data of various kinds. Recently Benetton tried to embed such a device in each item of clothing. At the moment this decision has been abandoned due to the protest campaign led by customer associations around the globe. See [30][31].

[11] It will be interesting to investigate the real effects of such systems and the oppositions they have triggered off. Every knowledge management system is, by definition, a documental

As individuals we can try to boycott the surveillance system if we are aware of being monitored. At the same time we are the same people who go to buy millions of video cameras or global positioning systems in order to know in every instant where our wife, husband, son or daughter is.

Do you remember the virtuous circle economics? This is exactly the reverse: a vicious circle that initially may cause a social block and then to follow an economic one. But what kind of economy is possible in a socially blocked system?

4 Security as control infrastructure or community infrastructure? Surveillance and connection sense

As David Lyon [17] suggests surveillance infrastructure is produced by the weaving of one to one marketing technologies with governmental agencies' improvements in tracking citizens[12]. This permits several subjects to track and influence each individual, simply by putting together the various pieces of the puzzle that, globally, represent his or her digital image: his or her own *body data* [17].

However this is only the beginning of the story. Today surveillance has become a mass phenomenon that crosses, and sometimes drives, the institutional side of it. The market dimensions are too big and too granular to place all the blame on the institutional infrastructure alone.

One hypothesis, that will be an interesting research path, would be to verify if this process may facilitate the diffusion of the sense of connection as a substitute for the sense of loss of community membership in our postmodern society. As some authors suggest (see De Kerchove, Carboni [7][9]) we are on the way to finding a *connection sense* - as the membership sense incomer - that, ipso facto, seems to be a weak tie. Maybe this concept could find a stronger dimension within a network communications system which has been founded, as it seems to be, on surveillance.

5 'Controlled Computing' and surveillance. The technical specifications and the log files issue: the core of the debate. Toward 'Surveillance Computing'

Despite what our opinion may be, the surveillance building system has started and it is irreversible. The surveillance infrastructure will be the ring which will connect the real world with the cyber world. Surveillance, in fact, is exerting its influence through the *body data* located in the cyber world of databases: its effects are very real indeed. Surveillance acts on real physical bodies: ours.

Allowing individuals to gain control of surveillance is perhaps the only way for this system to be accepted and to be maintained inside the democratic space as we know it.

---

and process surveillance system.

[12]There are many titles about this subjects. For example see Peppers & Rogers [26].

As Whitfield Diffie [20] asserts:

> 'To risk sloganeering, I say you need to hold the keys of your own computer'.

Actually this is a slogan and like most slogans it does not contain the whole story. The second part of the story, in fact, is that what we need are the keys to our own computer AND the permission to gain access (potentially) to the log files where every part of our *body data* lies [13].

> In other words we need to know who is doing what and when with our own *body data* and to do this we need to have access to the log files.

This possibility may allow us to again have the right to be in control of our *body data*. Obviously this is just the beginning, and by itself it is not enough. What is necessary is to translate this assertion into technical specifications that can prove it is a real aim. These technical specifications can be compared with those of various 'Controlled Computing' organizations (TCPA, TCG, etc..)[14].

This principle is based upon two facts:

1 the surveillance process belongs both to society and technology in a reciprocal manner;

2 it is possible to define technical specifications which will embed faith as a value within the technological systems our society is producing. These specifications are based on the right to gain access to ourselves: we want to own the property of our *body data* and to know the reputation of who, apart from us, has the right to gain this access.

The first point belongs to the continuous feedback that exists at every moment between society and technology. The second, on the contrary, belongs to what is possible. From a technical point of view this means that the cryptographer scientists decide to define the technical specification that makes it possible to pursue the second aim. This will stop criticism[15] about how bad 'Control Computing' is and help the action to start[16].

Here the important aspect is to prove that a 'Surveillance Computing' model is possible and that it can cope on equal terms with the 'Controlled Computing' model.

[13] See Carl S. Kaplan in [11].

[14] To know all the story related to the 'Controlled Computing' consortiums and their evolution see [1].

[15] However revealing what lies down this trend has been truly important indeed. Many of the changes which have taken place from last year to date have been caused by such revelations about TCPA and Palladium. See [2].

[16] One possible path of research could be to embed a personal backdoor, inside each one separate piece of body data. At least of the most important of the puzzle. One backdoor that starting from the principle at the root of digital signature connects each document to its real owner and allows one to gain access to the log files of the process in which it is involved by third parties.

This vision recognizes the surveillance stream which is flowing inside society, but does not fight it, rather it simply offers new ways to express itself. In this way we can see how an infrastructure which embeds the values of faith and sharing builds up an open social system in which, perhaps, some new economic movements may start again.

In this scenario there is no more static control over each *body data* as privacy rights supporters claimed in the past with no results.

A passive attitude has been transformed into an active one: concrete surveillance on our own *body data* that are available to our environment, but whoever gains access to them needs to give proof, in every instant, of his own reputation. This builds up, furthermore, a public responsibility process.

> To allow someone else to gain access under surveillance to our *body data* means there is no withdrawal. Data is still available but everybody holds the surveillance key, in person and through the community[17]. The possibility of sharing still exists and an economy based upon knowledge sharing is still possible, actually it finds a truly *secure* environment in which to grow.

The steps we can highlight are:

1 The definitions of the technical specifications needed to gain access to the *body data* log files.

2 The creation of a consortium which is capable of assembling this specification and which constitutes a first group of companies at hand to implement it.

3 The lobbying of legislators and positive actions through consumer associations.

To proceed towards 'Surveillance Computing' it is necessary to establish specifications and organizations. It is necessary to set up a technoeconomical institution that creates technical specifications and lobbying, coping face to face with TCPA or TCG etc.

6 Beyond privacy with real 'Trusted Computing'. Think different

If we really want to go towards a new concept of surveillance it is not possible to remain with archaic concepts like privacy[18]. Furthermore privacy takes with it the idea of distrust that goes exactly in the opposite direction in respect to what we have said till now. We need to overcome the traditional privacy borders

[17] Reputation is a social process.

[18] Privacy, as we know it, is historically defined: it has not always existed and, furthermore, is strongly influenced by the social-cultural context in which we consider it. Actually, today, it does not exist anymore. Thanks to Dr. Andrea Glorioso for this contribution.

inventing a new way to allow access to shared data in an open economy. This is why even some strong privacy rules, like in the EU[19], are not aimed in this direction.

The main principle is to define specifications of small groups of data, we can call it *body data core* that embeds an owner's digital signature. The possibility of gaining access to the log files has to be through this signature. Introducing a *body data core* simplifies the process because the log files need to be recorded only when external data are linked with someone of the core. For example: it is not necessary to gain access to the license plate image archive, but it has to be possible to have access to log files when the digital information embedded in the license plate image is used to gain access to some other core data. The *body data core* are in a process where every access to them triggers a record (embedding the owner's digital signature) in a log file. Obviously this is not a solution but just a very short example on the direction we can go if we decide to use the 'Trusted Computing' available technologies and use them in a different way in order to build a 'Society's Communications System' that embeds values rather different from today's concepts. This is not Utopia, unless you consider standards, protocols and specifications as Utopia [22].

These ideas are simple proposals for approaching the upcoming scenario, the network operating system. At the moment we are at a crossroads, in one direction there is only technology and in the other, there is the issue of privacy. These two directions lead on one hand to 'Controlled Computing' and on the other the old way of safeguarding privacy. Neither is fertile by itself: opportunities come from both sides. Considering them in such a way may generate, perhaps, a new developing path rich in consequences that up to now have not been possible to predict.

[19]This is a general consideration that, obviously, is not related to the various legislation within each individual EU country.

References

[1] Anderson Ross, Cryptography and Competition Policy - Issues with 'Trusted Computing', 2nd Annual Workshop on Economics and Information Security, May29th-30th, 2003

[2] Anderson Ross, 'Tcpa/Palladium Faq', at
www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[3] Anderson Ross, Security Engineering - a Guide to Building Dependable Distributed Systems, Wiley, 2001

[4] Hawken Paul, Amory Lovins and Hunter L. Lovins, Natural Capitalism. Creating the next industrial revolution, Little Brown an Co., Boston, 1999

[5] Betts Mitch, The future of business Intelligence, at
www.computerworld.com, April 14, 2003

[6] Capra Fritjof, The Hidden Connections, .The Hidden Connections: Integrating The Biological, Cognitive, And Social Dimensions Of Life Into A Science Of Sustainability, Random House Inc, 2002

[7] Carboni Carlo, La Nuova Società, Laterza, Bari, Italy, 2002

[8] Charny Bern, Nokia camera send a cell message, at
www.businessweek.com/technology/cnet/stories/997228.htm

[9] De Kerckhove Derrick, Brainframes, Technology, Mind and Business, Bosch & Keuning, 1991

[10] Farmer Dan and Mann Charles C., Surveillance Nation part 1, April 2003, MIT Technology review, at
www.techreview.com

[11] Farmer Dan and Mann Charles C., Surveillance Nation part 1, May 2003, MIT Technology review, at
www.techreview.com

[12] Locke Christopher, Gonzo Marketing. Winning through worst practices, Perseus Publishing, 2001

[13] Lessig Lawrence, The Future of Ideas, Random House, NY, 2001

[14] Lewis S., 'How Much is Stronger DRM Worth?', 2nd Annual Workshop on Economics and Information Security, May29th-30th, 2003

[15] Luhmann Niklas, Vertrauen. Ein Mechanism der Reduktion sozialer Komplexitat, IV ed. Stuttgart, Lucius & Lucius, 2000.

[16] Lyon David, The Electronic Eye: the rise of surveillance society, Polity Press, Cambridge 1994.

[17] Lyon David, Surveillance society: monitoring everyday life, Polity Press, Milton Keynes, 2001.

[18] Mazoyer Frank, Il lucroso mercato della sorveglianza, Le Monde Diplomatique, settembre, 2001

[19] Maturana H. Varela F., El àrbor del conocimiento, 1984, ISBN 88-11-67481-6

[20] Merritt Rick, Cryptographers sound warnings on Microsoft security plan, EE Tiimes, April 16, 2003, at
www.techweb.com/wire/story/TWB20030416S0002

[21] Mitnick Kevin, The art of deception, Wiley Publishing, 2002

[22] Moore Thomas, Utopia, Penguin Classics, 1965

[23] Buckendorff,J. *An interview with Tim O'Reilly*, from The O'Reilly Network, 12/07/2002, at www.open2p.com/lpt/a/2920

[24] Ozzie Ray, Perspective: a mosaic of new opportunities, April 22, 2003, Cnet at http://news.com.com/2010-1071-997725.html

[25] Pena Charles V., Targetting terrorism or... privacy?, The Whashington Times, 25/11/2002, at www.whashtimes.com

[26] Peppers Don & Rogers Martha, The One to One Future: Building Relationships One Customer at a Time, Doubleday, 1997

[27] Searls Doc, Weinberger David, Worlds of Ends, at http://worldofends.com, downloaded march 10th 2003

[28] Betts Mitch, The future of business intelligence, April 14 2003, at www.computerworld.com/databasetopics/data/story/0,10801,80243,00.html

[29] Lerner Josh, Tirole Jean, The Simple economics of Open Source, National Bureau of Economic Research, 2000, at http://opensource.mit.edu/papers/

[30] Katherine Albrecht, Auto-ID: Tracking everything, everywhere, June 2002, at http: seattlepi.nwsource.com/business/116508_smarttags09.shtml

[31] Krane Jim, Benetton rethinks using 'smart tags' in clothes, Associated Press, April 9, 2003, at http://seattlepi.nwsource.com/business/116508_smarttags09.shtml

[32] Robin Wood, Managing Complexity, The Economist Books, 2000