LOGEION
Filosofia da Informação

ARTIGO
http://dx.doi.org/10.21728/logeion.2017v4n1.p129-153

TACTICAL MEMORY: THE POLITICS OF OPENNESS IN THE CONSTRUCTION OF MEMORY[1]

Sandra Braman
University of Wisconsin-Milwaukee
http://www.uwm.edu/~braman
braman@uwm.edu

Abstract

Those in the openness movement believe that access to information is inherently democratic, and assume the effects of openness will all be good from the movement's perspective. But means are not ends, nothing is inevitable, and just what will be done with openly available information once achieved is rarely specified. One implicit goal of the openness movement is to create and sustain politically useful memory in situations in which official memory may not suffice, but to achieve this, openness is not enough. With the transition from a panopticon to a panspectron environment, the production of open information not only provides support for communities but also contributes to surveillance. Proprietary ownership of information is being challenged, but there is erosion of ownership in the sense of being confident in what is known. Some tactics currently in use need to be re–evaluated to determine their actual effects under current circumstances. Successfully achieving tactical memory in the 21st century also requires experimentation with new types of tactics, including those of technological discretion and of scale as a medium. At the most abstract level, the key political battle of the 21st century may not be between particular political parties or ideologies but, rather, the war between mathematics and narrative creativity.

Keywords: Panspectron enviroment. Surveillance. Tatical memory

MEMORIA TÁTICA: A POLÍTICA DE ACESSO LIVRE NA CONSTRUÇÃO DA MEMÓRIA

Resumo

Os engajados no movimento de acesso aberto acreditam que o acesso à informação é inerentemente democrático, e assumem que os efeitos da abertura serão todos bons partindo do ponto de vista deste movimento. Mas os meios não são fins, nada é inevitável e aquilo será feito com informações disponíveis em acesso aberto uma vez obtidas, raramente está especificado. Um objetivo implícito do movimento de acesso aberto é criar e sustentar a memória politicamente útil nas situações em que a memória oficial pode não ser suficiente, mas para conseguir isso o acesso aberto não é suficiente. Com a transição do panopticon para um ambiente panspectron, a produção de informações e seu acesso aberto não fornece suporte apenas para as comunidades, mas também contribui para a vigilância. A propriedade da informação está sendo desafiada, mas aí há uma erosão da propriedade no sentido de se estar confiante no que é conhecido. Algumas táticas atualmente em uso precisam ser reavaliadas para determinar seus efeitos reais nas circunstâncias atuais. A conquista da memória tática no século XXI também requer experimentação com novos tipos de táticas, incluindo as de discrição tecnológica e de escala como meio. No nível mais abstrato, a batalha política fundamental do século XXI pode não ser entre partidos ou ideologias particulares, mas sim a guerra entre matemática e criatividade narrativa.

Palavras-chave: *Ambiente panspectron. Vigilância. Memória tática*

[1] Este artigo foi originalmente publicado em First Monday, v. 11. n. 7, June, 2006

“Memory is not just of the past,
it’s of the future, too.”
Douglas Woolf.

1 Introduction

The openness movement is driven by the belief that access to information is inherently democratic, and riven by the assumption that all of the effects of openness will be good from the movement’s perspective. But means are not ends, nothing is inevitable, and just what will be done with openly available information once achieved is rarely specified.

Information has many definitions — and all may be simultaneously in play — but its most fundamental is as a constitutive force in society (BRAMAN, 1989). One implicit goal, therefore, is to use open information to create and sustain politically useful memory in situations in which official memory may not suffice. Memory is key because it is infrastructure, the informational structure critical to the individual and collective identities from which all agency springs. To achieve this type of memory, though, openness is not enough. Information and knowledge, tools and processes, require additional attention. It is here, between openness and infrastructure, that we find the space for doctrine (establishment of constitutional and constitutive principles), strategy (identification of long–term goals), tactics (choices regarding how to achieve strategic goals in a specific context with particular resources), and logistics (the material support systems upon which tactics rely).

In this article the focus is on tactics, “an arrangement of procedure with a view to achievement of specific ends” (*Oxford English Dictionary*). The history of tactics is one of ever–expanding foci and frames. In the military, for example — the domain in which tactical thinking has been the most highly developed — this began with attention to the volume of materials (soldiers, bullets, and armor), and subsequently turning to the problem of accuracy in use of those materials, the processes by which accurate weapons are produced, industrial strength in support of weapons production, and “Big Science” to improve industrial strength and generate weapons innovations (BEAUMONT, 1994; VAN CREVELD, 1991). This history can be broken down into three stages of tactical evolution: clockwork, motor, and network (DE LANDA, 1991), with the last stage of particular interest from the perspective of the opportunities for tactical memory uses of openness in the first decades of the 21st century.

Information and communication have long been used for tactical purposes. Roman leaders carried detailed notes with them into the field (LEE, 1993), Napoleon established a special staff to collect tactical information, and the formal communications structures of diplomacy were established as the formal tactical component of an international system in which foreign relations was the strategic domain (TRAN, 1987). Indeed, a tactical unit in the military can be defined as an information processing machine because it must include a means by which information is transmitted through a formation from leaders to soldiers and back in order to function (DE LANDA, 1991). While the question of whether or not machines will ever achieve an autonomous sense of consciousness remains unanswered, Dewdney (1998) describes smart tactical weapons — weapons that incorporate their own intelligent targeting and launch systems — as our first created forms of consciousness because they just live through the "I am" moment and then self–destruct.

In recent years we have begun to find the concept of tactics useful for thinking about cultural matters, and about the role of communication in society. The adaptation of biotechnology so that it is "appropriate" for indigenous, or "people's," environments, has been described as tactical (Kloppenburg and Burrows, 1996). Tactical voting is one of the three classic examples of lying and cheating in economic theory (MOLHO, 1997). Melucci's (1997) argument that the loci of social conflicts have shifted in many cases from overt political action to the linguistic and architectural codes that organize information leads to appreciation of the roles of language, knowledge production, and memory as tactical matters. Tactical media practitioners deliberately operationalize this insight (GARCIA; LOVINK, 1997).

Here we explore three problems that confront those attempting to use openness to create politically useful memory in the current environment and three limits to the effectiveness of current tactics in play. These difficulties provide the parameters of what may turn out to be the most significant political battle of the 21st century, the struggle between mathematics and narrative form. Three tactical recommendations are offered in response. Taken together, it is hoped that this analysis will provide some stimulus for thinking about the possibilities of tactical memory.

2 Three problems

Much of the activity within the openness movement is directed at removing long–standing barriers to information access, or at those being newly put in place in response to contemporary security concerns. However, even when there is openness, there are problems at each stage of the processes by which memory is developed — collecting, owning, and using the facts.

Collecting the facts:

Jeremy Bentham's (1787) concept of the panopticon, popularized by Foucault (1979), is widely used to describe the nature of surveillance as a form of information collection in the contemporary environment. The concept as initially put forward included three elements. An architecture was suggested that allowed one person to monitor many persons simultaneously. The person watching was given an economic interest in the effectiveness of the monitoring. And those being watched could not see the watcher; because as a result it could not be known with certainty whether or not one was being watched at any given time, those being watched would be motivated to regulate their behavior at all times — in effect, watching themselves. Foucault–inspired analyses of have broadened the concept to include the dehumanizing fragmentation of the individuals into disparate informational elements. Common across all of these is identification of a subject to be the target of surveillance and then the establishment of a single monitor or an array of monitoring equipment that keeps the subject within its gaze.

Though the concept of the panopticon is regularly invoked in discussions of contemporary surveillance techniques, such as the use of video cameras to record activity in public places, Hookway (2000) argues persuasively that, instead, the panopticon has been replaced with the panspectron. In a panspectron, no surveillance subject is identified in order to trigger an information collection process. Rather, information is collected about everything and everyone all the time. A subject appears only when a particular question is asked, triggering data mining in information already gathered to learn what can be learned in answer to that question. While in the panopticon environment the subject knows that the watcher is there, in the panspectron environment one may be completely unaware that information is being collected.

When the concept of the panspectron was first introduced, a mere half dozen years ago, it may have seemed to many to have been "merely" theoretical, speculative, or at best predictive. Since that time, however, the use of familiar technologies such as video surveillance cameras has rapidly spread, new technologies such as RFID chips and ubiquitous embedded computing systems have come into use, and we are learning more and more about the practices and intentions of those involved with homeland and national security. Though in the past social and political values as translated into laws prevented maximization of the capabilities of digital technologies for the collection of information about individuals, for the nonce, fear of terrorism has trumped. Until and unless effective legal barriers are re–erected, which in turn will require a re–adjustment of power relations among branches of government and political parties, the panspectron is already a reality in areas such as electronic communications (including telephone calls) and financial records, and will increasingly become so in other aspects of our lives.

In a full panspectron, it is impossible to hide physically. Aerial surveillance using heat and other sensors can track movement through rooms in the home and identify the plants being grown, Internet service providers and other organizations are being pressured or required to maintain digital records of transactions and communications for at least two years, and RFID chips move with us through space. The privacy mechanisms that seem natural to us as biological creatures — turning off the lights and shuttering the windows, moving by night, whispering, hiding — are irrelevant although as organisms we still engage in these practices. In the digital environment, privacy, like invasions of privacy, is instead a mathematical matter. Those who are watching use algorithms to discern patterns and relationships that in turn identify specific observational targets, and algorithms are used again to track all of the activities, transactions, and communications of individuals once identified as of interest. Efforts to elude the panspectron, then, must also be mathematical, whether that is accomplished digitally (through, for example, encryption or anonymizing techniques) or behaviorally (by acting in a manner in which what one does is not discernible by the algorithms used for tracking and pattern recognition purposes).

The impacts of this development on our ability to use openness for tactical memory purposes are three. First, one–way surveillance when those surveilled are not even aware that information is being gathered generates a type of interpersonal relationship that was historically rare but has become increasingly dominant in the contemporary world (CALHOUN, 1991). Second, citizens have lost the ability to choose which information will be available to others and which will not. And third, information deliberately provided to selected others and to the public becomes additional fodder for the panspectron, a problem revisited in more depth below.

Owning the Facts:

The central thrust of the openness movement, of course, is to confront means by which public access to information is restricted, and those involved with open source software have made abundantly clear the importance of openness in the processes by which information and knowledge are produced as well. Both of these have to do with ownership in the sense in which it is most commonly used, the legal right of possession, a meaning the *Oxford English Dictionary* traces back to the 16th century. A second meaning of ownership came into use in the 1980s, however, that should also be taken into account by the openness movement — being or feeling responsible for the resolution of a particular problem or issue. There are three ways in which this type of ownership of the facts has become problematic for those working with tactical memory: the possibility that one's memory will become criminalized; the practice of deliberately falsifying, or 'perturbing,' statistical records; and, the legal release of the national security establishment from the requirement of accuracy in the data used to justify surveillance of specific individuals and consequent treatment of those individuals by the national security and criminal justice systems.

Misappropriation by memory. Trade secrets is a way of protecting knowledge based in unfair competition law rather than intellectual property rights, but the recent trend, beginning with the seminal U.S. Supreme Court decision for the current trade secrets regime *Kewanee Oil Company v. Bicron Corporation* (1974), has been to treat trade secrets as property. Almost a century ago, however, even the U.S. Supreme Court recognized that trade secrets have as much to do with relationships as with property (E.I. DUPONT DE NEMOURS POWDER CO. V. MASLAND, 1917). For a long time trade secrets law distinguished between transferring knowledge in tangible forms (for example, in documents and other records) and in the intangible form of personal memory. Because it is often impossible to identify the sources of the knowledge one holds in memory, and to separate protectable knowledge from unprotectable knowledge in one's memory, courts were willing to consider cases involving the tangible transport of trade secrets but would not accept cases based on accusations of infringement of trade secrets via individual memory (GLAHN; SHILLING, 2002).

As constant and ever–quickening cycles of innovation have become central to economic success in information industries characterized by frequent employee mobility, however, concern over inappropriate knowledge transfer between corporations has become more extreme. The legal consequence has been a set of twin doctrines that address alleged transfers of trade secrets in the intangible form of personal memory — "misappropriation by memory" occurs when such knowledge has actually been used in a new setting, and fears of "inevitable disclosure" allow companies to act simply on the suspicion that such a transfer might take place (HAMLER, 2000; LOWRY, 1988; SAULINO, 2002). In some cases the intention to use memory–based trade secrets of one firm on behalf of another is clear, as when the individuals in *Morlife v. Lloyd Perry* (1997) reconstructed a former employer's client list in order to use it for themselves. The issue is less clear when, as in the case of *SCO v. IBM* (currently set to go to trial in 2007), employees who moved from one corporation to another relied upon knowledge of open source code in both places (Rogers, 2003). Other cases have involved claims that disputed knowledge was gained over the course of a shared education and durable personal relationship, not trade secrets.

Though there are lots of different ways in which information accessed may be cognitively processed — or not — the documentation of access to potential sources of knowledge made possible by a panspectron environment will make it easier to levy charges of misappropriation by memory in future. This raises the threat of criminalization of memory, whether or not there was intentionality or conscious awareness of knowledge sources.

Perturbing the facts. While it is the point of databases to collect and make available accurate information, both privacy law and public opinion demand that those who do data mining do not invade the privacy of individuals in the process of developing analyses of the whole. One class of techniques developed in response to these concerns involves restricting queries in a variety of ways so that the combination of results from successive queries of data in the aggregate cannot yield information about individuals through the ways in which the results overlap. A second class of techniques involves literally falsifying the data itself, known as "perturbation." Approaches to perturbation include such techniques as swapping values between records and adding noise to the results of a query.

While acknowledging that perturbation degrades the quality of the statistics and admitting that the goals of providing high quality statistics and preventing the full or partial disclosure of individual details are mutually exclusive, a profusely cited work by Agrawal and Srikant (2000) further elaborates on a technique for perturbing data that adds and subtracts a random value from each individual record. Multiple iterations of producing a distribution based upon the resulting statistics are necessary in order to approximate with confidence the original distribution. Agrawal and Srikant emphasize that the distribution, but not the values in individual records, can be reconstructed in this way. Though it has been demonstrated that it is possible to retrieve original data from datasets distorted by adding random values (KARGUPTA, *et al.*, 2003) (thus vacating the purported utility of the technique for security purposes), and argued that not enough is known about the tradeoffs between data value and risk of privacy invasion (IYENGAR, 2002), work on this approach continues.

Certainly these efforts have stimulated new thinking about how privacy should be defined for databases and their content. Dwork (2006), for example, proves that the goal of ensuring that nothing about an individual should be learnable from a database that can't be learned without access to the database is actually unachievable, making this an unworkable definition of database protection. Chawla, *et al.*, (2005) start by defining privacy as protection from being brought to the attention of others. From both perspectives, the availability of auxiliary information — information that is available from other sources to those who query databases — significantly diminishes the ability to statistically protect that data in the collection itself. This work is undertaken by mathematicians, with little attention to either legal or sociological analyses of the consequences of the effects of the approaches with which they are experimenting beyond the barrier question of the extent to which any given approach can effectively protect privacy. The work of philosopher Nissenbaum (2004) stands out in this literature for its inclusion of social theory and empirical evidence from the social sciences in her concept of contextual integrity — achieved when normative and distributive expectations are met in any given circumstances — for analysis of privacy threats from public surveillance.

Still, however, this step forward leaves a serious analytical lacuna in thinking through the ramifications for perturbing the data from a legal perspective, for loss of privacy is only one of the dangers that can arise for individuals from databases. Because access to resources and life opportunities often depends upon information in databases, several of the 18 data privacy laws currently in effect in the U.S. include a provision that offers opportunities to individuals to correct database errors when they are discovered. And in the current homeland security environment, the provision of inaccurate information to a database is defined as a terrorist activity. What provisions are in place to ensure that perturbed data at the individual level do not remain linked to the individual? How can individuals learn whether or not data about themselves in a database was perturbed after the point at which the accuracy of the information was checked? Tactical memory efforts can be undermined if data used for decisions–making purposes is deliberately altered in this way precisely because it is being made available.

Abandonment of the FBI accuracy requirement. In the homeland security environment, the Federal Bureau of Investigation (FBI) has an expanded mission that now includes national security matters as well as those of criminal justice, and a significantly eased situation regarding its ability to surveil. The National Crime Information Center (NCIC), created in 1967 to track criminal activity, is a key source of information that guides surveillance practices. In 1974 (with passage of the first U.S. Privacy Act), the FBI was required to assure the accuracy of the data it held, and in 1976 that database became computerized. However, in March of 2003, the Justice Department exempted the FBI's National Crime Information Center, along with its Central Records System and the National Center for the Analysis of Violent Crime, from the Privacy Act. This exemption was justified by the claim that it was necessary in order to avoid interference with the law enforcement functions and responsibilities of the FBI[2]. The Justice Department further claimed that the accuracy requirement should be dropped because it was impossible to determine in advance which information is accurate, relevant, timely, and complete.

This again creates a situation in which more information is available — at least to those in the security and criminal justice establishments — but the accuracy of that information drops in what can lead to a cascading chain of faulty processes of information collection. In worst–case scenarios, the ultimate result can be court cases in which this type of information is being used as evidence against the accused but — if collected under the provisions of the USA PATRIOT Act — the accused will not even be presented with an opportunity to know what evidence is being used or to challenge its facticity. Here the tactics of memory are clearly being used for strategic purposes.

Analogy and the law. Contemporary uses of analogy in legal thought are a good example of ways in which historically respected techniques can be inventively turned to new uses if there is political will. Analogy has long been considered a hallmark of legal reasoning even though analogical arguments are more persuasive than they are analytical (WEINREB, 2005). Deductive arguments can be subjected to the rules of formal logic and their conclusions empirically tested, as can the conclusions reached by inductive arguments, but analogical arguments are neither formally testable nor empirically verifiable. We have not developed techniques for evaluating the validity of analogical arguments, nor for determining the relative strength or weakness of any given analogy. Thus despite their importance in legal thought, formal models of legal decision–making and analysis instead focus on the tension between rules and standards. Still, analogical reasoning has been critical to legal thought because it provides a way for the law to grow and change in conformity with community views (LEVI, 1949), it is a way of achieving a conclusion even when fundamental aspects of a case or problem may be only partially theorized (SUNSTEIN, 1996), and it valuably serves

[2] *Federal Register*, 2003, pp. 14140–14141.

when the pragmatic limit of social scientific knowledge is reached but a legal decision is still required (GEERTZ, 1983)[3].

In periods of open political revolution, those who come into power feel free to abandon parts or all of the pre–existing legal system. When significant or radical political transformations take place under the guise of business as usual, however, analogy becomes particularly valuable as a means of adjusting the legal system to new political realities. The concept of functionally equivalent borders is a recent U.S. example of how this can be done.

It has long been held that the Fourth Amendment's restrictions on searches don't apply to those entering the country; anyone can be subjected to routine and nonroutine searches at the border without a warrant and without any requirement to show "probable cause" (evidence of reasons to suspect illegal behavior). Though geopolitical borders can be marked precisely, in the 1970s courts began to use an "elastic border" notion because, it was argued, it was not always possible to conduct searches at the border itself (SIMS, 1977). In 1973 the U.S.

Supreme Court replaced the elastic border notion with the concept of a functionally equivalent border (ALMEIDA–SANCHEZ V. U.S.). The concept was not clearly defined, requiring only that a search have some relationship to an international boundary (ITTIG, 1973). Roving border patrols, the notion of an "extended border search," the assumption that an illegal alien is always at a border, and the development of free trade zones in each state provide additional flexibility in use of the concept.

Since 9/11, concerns about U.S. citizens who have relationships with foreign nationals suspect because of their own social networks introduces a border nexus into any related investigation. In order to ensure that dangerous people or materials do not enter the United States, the federal government now requires searches to take place in foreign ports and airports before transport to the country begins, effectively exporting the U.S. border around the world. And in 2005, Congress explicitly interpreted the Homeland Security Act of 2002 as giving permission to the Department of Homeland Security (DHS) to exempt itself from U.S. law if deemed necessary in order to protect the border — in essence placing the DHS above the law[4].

Locations of geopolitical examples have long been examples of open information, but with this series of analogical and legal steps what we believe we know may no longer be so.

[3] More cynically, Richard Posner (2002) admits that lawyers find analogical arguments irresistible because they allow attorneys to limit their reading to law books.
[4] H.R. Conf. Rep. No. 109–72, 109th Cong., 1st Sess. 170–172 (2005).

With loss of the meaningful ownership of this type of open information, our ability to construct memories about cross–border relations declines and we are less able to use memory in politically effective ways.

Inference attacks. There is a long history of classifying information, but in recent years there has also been growing interest in the category of "sensitive but unclassified" (SBU) information — information to which the public has access but that can, in combination with other information or within a certain context of understanding, yield insights considered undesirable. To those in the national security establishment, the ability to generate such inferences is understood to be a form of attack. As described by computer scientists working to protect the security of single databases, an "inference attack" occurs when a user can derive an answer to an unauthorized question on the basis of the results of an authorized query. Those results may be positive (information produced) or negative (information that is not produced in response to a query) (ISHIHARA, *ET al.*, 2005). Interoperability between databases and other forms of data sharing across organizational boundaries increase the potential for such inferences (MITRA, *et al.*, 2006). And because knowledge held by those who access data is key to the ability to draw inferences, the expanding universe of open access information — the goal and the result of the openness movement — again increases the danger of what are being defined as inference attacks.

Three classes of policies for protecting against inference and aggregation attacks are being publicly discussed (STRICKLAND, 2005). There are policies that structure the information itself, policies that structure access to information, and policies that rely upon intermediaries for secure information sharing. The first class includes compartmentalizing data of different types whether via metadata tagging or the erection of internal database barriers; filtering or disguising data (including through the use of perturbation as discussed above); and, finding ways to identify data that might be sensitive given certain lines of inference. The second class includes traditional vetting and need to know approaches to determining who should be allowed to access certain data, relying upon roles to define who should have the right to know what information as circumstances shift, and event–triggered access as the most dynamic approach. The third class includes release controls such as vocabulary limits; secure multiparty computing that requires successful completion of joint functions in order to obtain a correct output; the use of multidimensional classification systems; and, a variety of ways of combining these approaches.

Techniques for detecting the potential for inference include identifying diverse tags that can be mapped onto the same concept in an ontology ("ontological equivalence") (KAUSHIK, *et al.*, 2005) as well as analyzing logical, semantic, and mathematical relationships (STRICKLAND, 2005). Memory–based reasoning can also be turned to this end. Those engaged in this activity, however, face a number of difficulties: more than one chain of inference may be involved in achieving any given conclusion. Relationships among data may derive from database design rather than explicit compartmentalization or tagging of the data. It may be possible to achieve a partial inference that has a reasonable degree of probability even when absolute certainty is not achieved. Most importantly, it is impossible to fully control for the user's domain knowledge; as a result, speculation regarding which information needs to be protected in order to prevent a certain type of inference from being developed may be completely inaccurate.

The last of these is of particular interest to those in the openness movement, for considerable effort is going into expanding the domain of user information that can be modeled in order to determine possible lines of inference. There has been considerable public debate about the increase in the collection about personal information, including such details as the Web sites one visits, since 9/11, and about the abandonment of barriers to the data matching across databases. These legal developments, in addition to the proactive efforts of those in the openness movement, continually expand the universe of information that can be mined for possible inference attacks.

3 Three limits

A number of current political tactics take advantage of — or insist upon — increased opportunities for openness in access to information and the processes of knowledge production. Voluntary exposure, efforts to democratize decision–making about scientific research and the uses of that research, and engaging in ephemeral rather than permanent actions and relationships are three such tactics. What are the strengths and weaknesses of each of these uses of openness in the face of the problems identified above?

Voluntary Exposure

A decade ago we began to see the first experimentation with voluntary exposure as a means of creatively responding to encroachments on personal privacy with the Jennie–cam and other adventures involving constant recording of oneself or one's environs and the distribution of that information over the net. Today these have moved from the realm of the artist into everyday life; individuals share their personal cell phone calls loudly in public places, display intimate details about themselves regularly on MySpace, and publish their diaries or political thoughts as blogs. The term "sousveillance" has come into use to distinguish such practices from the involuntary exposure generated when surveillance is undertaken by others.

Most of this activity no longer carries an explicit political valence, but some of it does. Blogs offer a premiere example of voluntary exposure that is deliberately intended to counter perceived biases in media reportage about important political events and barriers to information flows about political realities, activities, and preferences on the ground. Global Voices (www.globalvoicesonline.org), for example, is a highly sophisticated Web portal hosted by the Berkman Center for Internet and Society at Harvard Law School that offers access to blogs with news and political analysis from around the world. Managed by a former news agency bureau chief, this site is a boon to readers, who can trust the multiple layers of gatekeeping involved in choosing which bloggers to present from the myriad in any given region or on a particular topic. Growth in relationships among blog–active non–profits, effective social and political action driven by bloggers, eager participation in blogging conferences, and repeated take-up by the mainstream media of news stories and information first introduced in blogs (see, *e.g.*, LAWSON–BORDERS; KIRK, 2005) all provide evidence that this site and related blogging activity are successfully taking advantage of the Web to enhance the diversity of information about political affairs and support the building of community among those with shared political views.

While blogs have enriched the public sphere, though, they are also themselves subjects of analysis. The intelligence community is deeply interested in bloggers representing a diversity of positions along the political spectrum in various parts of the world. For this community, blogs and blog portals like Global Voices provide an extremely efficient way of identifying individuals and groups of political interest as well as content that can be mined for data and possible lines of inference as part of the knowledge domain that constitutes the panspectron. It is possible that these uses of the voluntary exposure offered by the blogosphere could undermine the intentions of some of those who understand what they are doing to have a particular set of tactical uses in the political environment.

Openness in Knowledge Production

Wikipedia is one successful example of use of the Web for open knowledge production, and there are others. While there are critiques of this approach to participatory knowledge production, these share many features with critiques of other ways of producing information, and both techniques and norms for responding to criticisms and weaknesses are still developing. Compared to "Big Science," however, this process might be described as "small" in the sense that knowledge is contributed by individuals who voluntarily enter the conversation with what they bring to it and who refine that knowledge as a result of discussion with others who have also brought what they know to the table. In contrast, Big Science involves large amounts of money, highly developed organizational and experimental structures, many people engaged in coordinated collaborative activity, and hierarchical decision–making regarding which questions will be asked. The phrase "post–normal science" refers to the openness movement as it has engaged with Big Science.

The concept of post–normal science was born in environmentalism. The history of political protests against specific paths of scientific research goes back several decades in various forms of resistance to university acceptance of government funds for research in areas such as the development of nuclear weapons. It was fear over the release of genetically modified (GM) organisms into the environment, however, that stimulated the development of calls for participatory, or post–normal, science (MURDOCK, 2004). The ideal put forward by proponents of post–normal science is democratic decision–making about which large–scale scientific research governments would fund, as well as about how the results of research would be used.

Most of those calling for post–normal science, however, focus on the effects of the uses of research results but direct their demands as well at research processes, conflating policy– making and knowledge production. If the ideal defined as "openness" were acted upon, the actual result would be closure of many important types of basic research. The notion of incorporating values and social preferences into research funding decisions is a good one, but doing so requires more than the one–step call for openness, and questions about the ethics and politics of uses of research results must involve quite other processes in order to be effective.

The Ephemeral

Another tactic being used by those who are struggling to find effective modes of acting politically in the contemporary environment has been to engage in ephemeral rather than programmatic actions, and to build temporary rather than stable and enduring relationships and organizations. In a panopticon environment, these would be effective techniques. In a panspectron environment, however, this detail can become additional information for data mining.

The ephemeral is one form of the statistically improbable, a notion that has already been turned into a marketing tool by Amazon, which provides information on its Web site about the "statistically improbable phrases" that appear in books it sells. While poets since ancient times have striven to produce statistically improbable language in the form of unique expressions, in the panspectron tracking the use of such phrases allows another form of inference tracking.

National security implications of the statistically improbable were introduced in the early 1990s, when "new security theory" was developed to cope with what were believed then to be post–Cold War conditions. One of the big problems for new security theory was identifying the enemy when the Soviet Union and communism no longer served, and in response four categories were identified: terrorists, those involved with drugs, those who economically threatened the U.S., and those whose behaviors were statistically unpredictable (STEELE, 1990). Against this context, then, the very effort to act or relate in ephemeral ways as a tactic that takes advantage of an open environment can serve to draw attention to one's activities as a potential danger to the state. Meanwhile, when attorney general, John Ashcroft put forth the goal of building a national database that would include six degrees of separation in the information recorded. If this goal were reached, individuals on six different flights who sat in the same airplane seat, or six different renters of a particular apartment, would be linked even though in almost all such cases the relationships would be spurious.

4 Three recommendations

This brief investigation into threats to openness and weaknesses in tactics believed to take advantage of openness point to a dilemma for the openness movement: all structures of open content, all uses of open content, and all processes by which open content is acquired, developed, or created, are voluntary contributions to the panspectron that can then in turn be mined for analysis of possible inference attacks and identification of individuals who might be considered politically dangerous. This fact does not lead to the conclusion that openness is not desired, but it does suggest the need to develop additional tactics appropriate to the current environment. We can call these the techniques of tactical memory because they create and sustain politically effective memory. They include treatment of scale as a medium, technological discretion, and collaboration.

Scale as Medium

Mandelbrot's (1977) visualization of fractals, forms that appear to be highly irregular at any single scale but which are self–replicating across scales, has helped us literally see how scale is a medium in itself. Learning to write offers an introduction to this notion as we first put letters into words, then words into sentences, sentences into paragraphs, and paragraphs into an overarching narrative structure. Thinking about genre, channels, and mediums in the digital environment has made grammatical relationships among these visible. We use the word grammar to refer to the construction of the sentences that are textual elements. Genre is in essence the grammar of narrative structure. Channels entail programming grammars within a given medium. Media are distinguished from each other by the grammar of their channels. In the pan–medium environment (THEALL, 1999), distinct media, each with its own reach, types of access and borders, scale and scope, provide one grammar for our communicative and informational activities, and the emergent information architectures provided by semantic Web–type ontological efforts provide another. And scalability, of course — the ability to scale up a process or activity in terms of amount of information being processed or transmitted, the geographic or chronological reach of access and distribution, and/or the numbers of people simultaneously involved in content production and use — is a key evaluative criterion for digital content and processes.

Information search and collection systems each have their own scale, and the term granularity is used to refer to the scale of the datum–collecting mesh in use by any given system. Ulrich Beck (1992) examined the political ramifications of this when he powerfully uncovered inadequacies of the information collection mechanisms of the modern state in a world in which the critical causal mechanisms often cross boundaries of geopolitics, time, and organizational form; involve numerous causal mechanisms that interact in complex ways; and, may yield results that are themselves currently imperceptible. Schwenkel (2006) offers an example of the role of scale in the construction of memory with political value in her analysis of the way in which interpenetrated and transnational memories affect understandings of the history — and therefore the present — of Vietnam. These features, however, also offer tactical possibilities if scale is understood as a grammar in itself. Because the mathematical techniques used to guide surveillance mechanisms and tomine data will each have their own granularity, continuous redesign of scale could provide relief from the algorithmic eye.

Crossing scale can be treated as a medium in itself. In this domain artists may be the leaders in developing tactical memory techniques.

Technological Discretion

Discretion is the space between what is intended, or possible, and what is actually done. Utopian visions of the changes to be wrought by new information technologies often founder on their failure to distinguish among the technological potential at the cutting edge of innovation in resource–rich situations (what we might call the technological horizon), what is logistically available to any given individual or community (the technological environment), and what is actually used by that individual or community[5]. In the moments in which choices are made in the formation of one's own information ecology vis–à–vis the potentials of the information environment, tactical decisions are possible. That discretion can be exercised both with new technologies, and with old.

The most obvious forms of technological discretion are the opportunities to choose which technologies one will engage in one's personal ecology, and how. One can choose to be networked all the time — or only a few minutes a day when actively communicating, perhaps from equipment devoted to this purpose alone. One can choose to be exposed to push media (such as that offered by television broadcasters), or pull media alone (choosing reading material or the Web sites one surfs). One can carry a GPS–enabled cellphone at all times, being constantly available for voice contact and visible to geographic location mechanisms, or not. Appreciation of the power in refusing to take up a technology suggests that some data analysis — and some policy goals — should be reconsidered.

Designers of new technologies have specific uses and effects in mind, but each also has unintended affordances. Experience in the digital environment, in fact, has invested the concept of affordances with new meaning. A relatively young word — the *Oxford English Dictionary* notes its first appearance only in 1879 — the concept has had its most active use among psychologists who, following Gibson (1966), have used it to refer to what organisms can perceive of an object's characteristics from the perspective of what they can do with those features. Optical information that shows an object to be rigid, flat, level, and extended, for example, will be interpreted as something upon which one can stand or sit. In today's environment, the notion of affordances has been taken up (see, *e.g.*, DE LANDA, 1991) to refer to new forms of utility individuals and groups discover as they play with the digital

[5] What Nardi and O'Day (1999) usefully named the information ecology.

potential. E–mail itself developed out of the experience of scientists who used the affordances offered by a network established to exchange scientific data when they found that communicating interpersonally about that data — and then, in turn, about themselves and social affairs — improved their ability to conduct scientific analyses (ABBATE, 1999). Over the past two decades, an entire culture has been built up devoted to exploring the affordances of the network environment, whether for the positive and creative purposes of hacking or for the more destructive ends of cracking. Discoveries made by those engaged in this activity have been so important that the scholarly literature on R&D now acknowledges that valuable innovation can be undertaken by users, and that what in the past had been described as misuses of technologies or failures to diffuse are in fact often moments of adaptation or a continuation of the innovation cycle.

Discretion can also be exercised to develop new uses of old technologies. The ancient practice of moving earth for purposes of ritual communication and scientific knowledge production is appearing again in contemporary art. The concept of spandrels, most commonly heard in discourse about architecture, refers to design features that have lost their original functions but that are still in use for aesthetic or other communicative purposes; an example of discretion in the use of a spandrel for purposes important to the sustenance of memory was the practice of hiding forbidden manuscripts inside of the bindings of books, where they often remained for many hundreds of years before being rediscovered, enabling lost history to be regained. Storing information in the "underwriting" of palimpsests, media that have been written upon, erased, and written upon again, is as ancient as the use of the wax tablets from which the term derives but as newly available as storing critical information on hard drives in files that have been erased and overwritten, or in edits ostensibly removed from documents. Christopher Dewdney (1998) tells the wonderful story of the use of what he calls "Maginot Line" technologies when Persian rug–makers were able to use their skills in building coherent patterned wholes out of small fragments of material to reconstruct U.S. government documents destroyed by the CIA when the Shah of Iran fell.

Collaboration

Some of the oldest techniques of all remain valuable in the 21st century. Though asking two people with no pre–existing relationship to collaborate on building a consistent memory of an event may not yield results any better than what would be generated by each individual working alone, when friends are asked to engage in this exercise stronger, more detailed, and more coherent memories emerge (ANDERSSON; RÖNNBERG, 1996). The effect is strengthened yet again when couples who have been married a long time are asked to report on shared memories; together, these couples do better on memory performance tests than many individuals who are much younger (Bower, 1997). Collaborations are also required in order to achieve success with many of the other techniques discussed above; in this sense, the distinction between individual and collective memory begins to fall away. The implications for tactical memory are obvious: Sustain social networks over time. Collaborate on memory activities (downloading and circulating key documents, for example). And multiply content sites so critical memory can't be destroyed. Such collaborations may also extend to developing a sense of that which should be public memory and that which remains private. In many cultures there are distinctions between memories that you admit to, and those which are kept secret for tactical reasons. Just where to locate particular memories should be a critical part of our reconsideration of the boundaries between the public and the private in the 21st century.

The new twist on collaboration today, however, is that often the tools through which it is exercised are themselves digital in nature. This fact presents another challenge to those in the openness movement, for the software that supports specific modes of doing business and that enables interpersonal and group communications can itself now be patented.

5 One dilemma: mathematics vs. narrative creativity

> "Poets are marching again upon
> the hills of history."
> Ed Sanders.

Openness, yes, but openness is only the beginning of the processes by which information acquires meaning and fulfills its role as a constitutive social force. The use of open information to build and sustain tactical memory, based on community experience rather than official fiat and self–consciously devoted to providing the infrastructure for effective political action, is implicitly one of the goals towards which the openness movement strives. While there is a rising tide of support for openness in many venues, there is also an array of practices and principles in play. With the transition from a panopticon to a panspectron environment, the production of open information becomes a contribution to surveillance efforts in addition to offering means by which communities can achieve their own goals and engage in public discourse about shared matters of public concern. Proprietary ownership of information is being challenged, sometimes successfully, but there is erosion of ownership in the sense of being confident in what is known: the effective location of something as basic as that of a geopolitical border has become elusive and unknowable, actions based on memory may be treated as illegal or a threat to national security simply because one's memory is involved, even official bodies are deliberately "perturbing" facts specifically because of openess, and the national security establishment need not require accuracy from the information it uses to identify individuals to be treated with suspicion.

All of the reasons why open information is desirable remain valid and openness continues to be a goal worth pursuing with energy. For purposes of tactical memory, though — community–based memory that can provide a foundation for politically effective action — some political tactics currently in use should be re–evaluated to determine their effects under current circumstances rather than as they may have worked under conditions of the past. The very traditional tactics of collaboration remain valuable, but it is also important to experiment with new types of tactics specific to the digital and network environment, including those of technological discretion and of scale as a medium.

At the most abstract level, the key political battle of the 21st century may not be between particular political parties or ideologies but, rather, the war between mathematics and narrative creativity. Data mining, searching for inference attacks, and surveillance are driven by mathematical algorithms. Against that context, it is narrative creativity, the ability to continually tell stories in new ways, that provides the means by which to elude the granularity and the logic of the mathematical nets used by those who would restrict public conversation and action to preferred forms.

REFERENCES

Janet Abbate, 1999. *Inventing the Internet*. Cambridge, Mass.: MIT Press.

Rakesh Agrawal and Ramakrishnan Srikant, 2000. "Privacy–preserving data mining,"*Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data*, volume 29, number 2, pp. 439–450.

Almeida–Sanchez v. United States, 413 U.S. 266, 272–73 (1973).

REFERÊNCIAS

ABBATE, Janet. **Inventing the Internet**. Cambridge: MIT Press, 1999

AGRAWAL, Rakesh; Srikant, Ramakrishnan. Privacy–preserving data mining. In: 2000 INTERNATIONAL CONCERENCE OF MANAGEMENT OF DATA, 29., 2000, Dallas. **Proceedings** … New York: ACM, 2000, n. 2, p. 439-450.

ALMEIDA SANCHES. Caso Almeida-Sanches versus Suprema Corte dos Estados Unidos, 413

	U.S. 266, 272–73, 1973. Disponível em: <https://supreme.justia.com/cases/federal/us/413/266/>. Acesso em: 25 ago. 2017.
J. Andersson and J. Rönnberg. 1996. “Collaboration and memory: Effects of dyadic retrieval on different memory tasks,” *Applied Cognitive Psychology*, volume 10, number 2, pp. 171–81.	ANDERSSON, J.; RÖNNBERT, J. Collaboration and memory: effetcs of dyadic memory task. **Applied Cognitive Psychology**, v. 10, n. 2, p. 171-181, 1996.
Roger A. Beaumont, 1994. *War, chaos, and history*. New York: Praeger.	BEAUMONT, Roger A. **War, chaos, and history**. New York: Praeger, 1994.
Ulrich Beck, 1992. *Risk society: Towards a new modernity*. Translated by Mark Ritter. London: Sage.	BECK, Ulrich. **Risk society:** towards a new modernity. Trad. Mark Ritter. London: Sage, 1992.
Jeremy Bentham, 1787. “Panopticon,” In: Miran Bozovic (editor). *The panopticon writings*. London: Verso, 1995, pp. 29–95.	BENTHAM , Jeremy. Panopticon [1787]. In: BOZOVIC, Miran (Ed.). **The panopticon writings**. London: Verso, 1995, p. 29–95.
Bruce Bower, 1997. “Partners in recall: Elderly spouses build better memories,” *Science News*, volume 11 (13 September), pp. 174–175.	BOWER, Bruce. Partners in recall: elderly spouses build better memories. **Science News**, v. 11, p. 174–175. Sept.1997.
Sandra Braman, 1989. “Defining information: An approach for policy-makers,” *Telecommunications Policy*, volume 13, number 3, pp. 233–242.	BRAMAN, Sandra. Defining information: an approach for policy-makers. **Telecommunications Policy,** v. 13, n. 3, p. 233–242, 1989.
Craig Calhoun, 1991. “Indirect relationships and imagined communities: Large–scale social integration and the transformation of everyday life,” In: Pierre Bourdieu and James S. Coleman (editors). *Social theory for a changing society*. Boulder, Colo.: Westview Press, pp. 95–120.	CALHOUN, Craig. Indirect relationships and imagined communities: large–scale social integration and the transformation of everyday life. In: Bourdieu , Pierre; COLEMAN, James S. (Ed). **Social theory for a changing society.** Boulder (Colorado): Westview Press, p. 95–120, 1991.
Shuchi Chawla, Cynthia Dwork, Frank McSherry, Adam Smith, and Hoeteck Wee, 2005. “Toward privacy in public databases,” presented to the Second Theory of Cryptography Conference, Cambridge (February), at http://theory.lcs.mit.edu/~asmith/PS/sdb-tcc-2005-almost-final-proceedings.pdf, accessed 9 August 2006.	CHAWLA, Shuchi et al. Toward privacy in public databases. In: THEORY OF CRYPTOGRAPHY CONFERENCE, 2., 2005, Cambridge. **Proceedings ...** Cambridge: Springer, 2005. Disponível em: <http://theory.lcs.mit.edu/~asmith/PS/sdb-tcc-2005-almost-final-proceedings.pdf>. Acesso em: 9 ago. 2006.
Manuel De Landa, 1991. *War in the age of intelligent machines*. New York: Zone Books.	De LANDA, Manuel. **War in the age of intelligent machines**. New York: Zone Books, 1991.
Christopher Dewdney, 1998. *Last flesh: Life in the transhuman era*. Toronto: McClelland and Stewart.	DEWDNEY, Christopher. **Last flesh**: life in the transhuman era. Toronto: McClelland and Stewart. 1998.
Cynthia Dwork, 2006. “Differential privacy,” presented to the 33rd International Colloquium on Automata, Languages and Programming, S. Servolo, Venice (July), and at	DWORK, Cynthia. Differential privacy. In: INTERNATIONAL COLLOQUIUM ON AUTOMATA, LANGUAGES AND PROGRAMMING , 33., 2006, Veneza.

http://research.microsoft.com/research/sv/DatabasePrivacy/dwork.pdf, accessed 9 August 2006.	**Proceedings ...** BUGLIESI, M. et al (Ed.). Automata, Languages and Programming. Spirng Verlang. Disponível em: <http://research.microsoft.com/research/sv/DatabasePrivacy/dwork.pdf> Acesso em: 9 Aug. 2006.
E.I. duPont de Nemours Powder Co. v. Masland, 244 U.S. 100 (1917). *Federal Register*, 2003, pp. 14140–14141 (24 March).	E.I. DUPONT DE NEMOURS POWDER CO. *v.* Masland, 244 U.S. 100 (1917). Federal Register, 2003, p. 14140–14141, 24 March, 1917.
Michel Foucault, 1979. "Panopticism," In: *Discipline and punish: The birth of the prison*. Translated by Alan Sheridan. New York: Vintage Books, pp. 195–230.	FOUCAULT, Michel. Panopticism. In:___ **Discipline and punish:** the birth of the prison. Trad.Alan Sheridan. New York: Vintage Books, p. 195–230, 1979.
David Garcia and Geert Lovink, 1997. "The ABC of tactical media," first distributed via the nettime listserv; now available online at http://subsol.c3.hu/subsol_2/contributors2/garcialovinktext. html, accessed 9 August 2006.	GARCIA, David; LOVINK, Geert. **The ABC of tactical media**. Disponível em: <http://subsol.c3.hu/subsol_2/contributors2/garcialovinktext. html>. Acesso em: 9 Aug. 2006.
Clifford Geertz, 1983. "Fact and law in comparative perspective," In: *Local knowledge: Further essays in interpretive anthropology*. New York: Basic Books, pp. 167–234.	GEERTZ, Clifford. Fact and law in comparative perspective. In: ____ **Local knowledge**: further essays in interpretive anthropology. New York: Basic Books, pp. 167–234, 1983
James Jerome Gibson, 1966. *The senses considered as perceptual systems*. Boston: Houghton Mifflin.	GIBSON, James Jerome. **The senses considered as perceptual systems**. Boston: Houghton Mifflin, 1966.
Wilbur A. Glahn and Cameron G. Shilling, 2002. "The cutting edge of trade secret law," *Findlaw.com*, at http://library.findlaw.com/2002/Dec/20/132443.html, accessed 9 August 2006.	GLAHN, Wilbur A; SHILLING, Cameron G. 2002. The cutting edge of trade secret law. **Findlaw.com**. Disponível em: <http://library.findlaw.com/2002/Dec/20/132443.html>. Acesso em: 9 Aug. 2006.
Nathan Hamler, 2000. "The impending merger of the inevitable disclosure doctrine and negative trade secrets: Is trade secret law heading in the right direction?" *Journal of Corporate Law*, volume 25 (Winter), pp. 383–405.	HAMLER, Nathan . The impending merger of the inevitable disclosure doctrine and negative trade secrets: is trade secret law heading in the right direction? **Journal of Corporate Law**, v. 25, p. 383–405. Winter 2000.
Branden Hookway, 2000. *Pandemonium: The rise of predatory locales in the postwar world*. Princeton, N.J.: Princeton Architectural Press.	HOOKWAY, Branden . **Pandemonium:** the rise of predatory locales in the postwar world. Princeton, N.J.: Princeton Architectural Press. 2000.
Yasunori Ishihara, Shuichiro Ako, and Toru Fujiwara, 2005. "Security against inference attacks on negative information in object–oriented databases," *IEICE Transactions on Information and Systems*, volume E88–D, number 12, pp. 2767–2776.	ISHIHARA, Yasunori; AKO, Shuichiro; FUJIWARA, Toru. Security against inference attacks on negative information in object–oriented databases, **IEICE Transactions on Information and Systems**, v. E88–D, n.12, p. 2767–2776.,2005
Judith B. Ittig, 1973. "The rites of passage: Border searches and the Fourth Amendment," *40 Tennessee Law Review 329 (Spring)*.	ITTIG, Judith B. The rites of passage: border searches and the Fourth Amendment, *40* **Tennessee Law Review***,* v. 40, Spring, 1973.
Vijay S. Iyengar, 2002. "Transforming data to	IYENGAR, Vijay S. Transforming data to satisfy

satisfy privacy constraints,” *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery* (New York: ACM Press), pp. 279–288.	privacy constraints. In: ACM SIGKDD INTERNATIONAL CONFERENCE ON KNOWLEDGE DISCOVERY*,* 8., Edmonton (Canadá). **Proceedings** ... KLEIM, Daniel, NG, Raymond (Ed.). KKD-2000. New York: ACM Press, 2002, p. 279–288.
Hillol Kargupta, Souptik Datta, Qi Wang and Krashanmoorthy Sivakumar, 2003. “On the privacy preserving properties of random data pertubation techniques,” *ICDM 2003: Third IEEE International Conference on Data Mining* (New York: IEEE), pp. 99–106.	KARGUPTA, Hillol et al. On the privacy preserving properties of random data pertubation techniques. In: IEEE INTERNATIONAL CONFERENCE ON DATA MINING, 3., Melbourne. **Proceedings …** New York: IEEE, 2003 pp. 99–106. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1250908>. Acesso em: 25 ago. 2017.
Saket Kaushik, Wijesekera Duminda, and Paul Ammann, 2005. “Policy based dissemination of partial Web ontologies,” *SWS ’05: Proceedings of the 2005 ACM Workshop on Secure Web Services* (New York: ACM Press),pp. 43–62.	KAUSHIK, Saket; DUMINDA, Wijesekera; AMMANN, Paul. Policy based dissemination of partial Web ontologies. In: ACM WORKSHOP ON SECURE WEB SERVICES, SWS, 5., 2005, **Proceedings…** SWS’5. New York: ACM Press, 2005, p. 43–62.
Kewanee Oil Company v. Bicron Corporation, 416 U.S. 470 (1974).	KEWANEE OIL COMPANY. Caso Kewanne Oil Company versus Bicron Corporation, Suprema Corte dos Estados Unidos, p.416-470, 1974. Disponível em: <https://supreme.justia.com/cases/federal/us/416/470/case.html >. Acesso em: 25 ago. 2017.
Jack Kloppenburg and Beth Burrows, 1996. “Biotechnology to the rescue? Twelve reasons why biotechnology is incompatible with sustainable agriculture,” *Ecologist*, volume 26, number 2, pp. 61–68.	KLOPPENBURG, Jack; BURROWS, Beth. Biotechnology to the rescue? Twelve reasons why biotechnology is incompatible with sustainable agriculture. **Ecologist**, v. 26, n.2, p. 61–68, 1996.
G. Lawson–Borders and R. Kirk, 2005. “Blogs in campaign communication,” *American Behavioral Scientist*, volume 49, number 4, pp. 548–559.	LAWSON–BORDERS, G.; KIRK, R. Blogs in campaign communication. **American Behavioral Scientist**, v.49, n. 4, p. 548–559, 2005.
A.D. Lee, 1993. *Information and frontiers: Roman foreign relations in late antiquity*. Cambridge: Cambridge University Press.	LEE, A.D. **Information and frontiers: Roman foreign relations in late antiquity.** Cambridge: Cambridge University Press, 1993.
Edward Levi, 1949. *An introduction to legal reasoning*. Chicago: University of Chicago Press.	LEVI, Edward. **An introduction to legal reasoning.** Chicago: University of Chicago Press, 1949.
Suellen Lowry, 1988. “Inevitable disclosure trade secret disputes: Dissolution of concurrent property interests,” *Stanford Law Review*, volume 40 (January), pp. 519–544.	LOWRY, Suellen. Inevitable disclosure trade secret disputes: Dissolution of concurrent property interests. **Stanford Law Review**, v. 40, p. 519–544, Jan. 1988.
Benoit B. Mandelbrot, 1977. *Fractals: Form, chance, and dimension*. New York: W.H. Freeman.	MANDELBROT, Benoit B. **Fractals:form, chance, and dimension.** New York: W.H. Freeman, 1977.
Prasenjit Mitra, ChiChun Pan, and Peng Liu,	MITRA, Prasenjit; PAN, ChiChun; LIU, Peng

2006. “Privacy preserving semantic dinteroperation and access control of heterogeneous databases,” *Proceedings of the 2006 ACM Symposium on Information, Communication, and Computer Security* (New York: ACM Press), pp. 66–77.	Privacy preserving semantic dinteroperation and access control of heterogeneous databases. In: ACM SYMPOSIUM ON INFORMATION, COMMUNICATION, AND COMPUTER AND COMMUNICATION SECURTY, 1.,2006, Taipei. **Proceedings…** New York: ACM Press, 2006, p. 66–77.
Alberto Melucci, 1997. *Challenging codes: Collective action in the information age*. Cambridge: Cambridge University Press.	MELUCCI, Alberto. **Challenging codes: collective action in the information age.** Cambridge: Cambridge University Press, 1997
Ian Molho, 1997. *The economics of information: Lying and cheating in markets and organizations*. Oxford: Blackwell.	MOLHO, Ian. **The economics of information:** lying and cheating in markets and organizations. Oxford: Blackwell, 1997.
Morlife, Inc. v. Lloyd Perry, 56 Cal. App. 4th 1514 (1st Dist. Aug. 14, 1997).	MORLIFE, INC. Caso Morlife, Inc versus Lloyd Perry, 56, 4a Corte de Apelação da Califórnia, 1514. 1st Dist. Aug. 14, 1997. Disponível em: <http://law.justia.com/cases/california/court-of-appeal/4th/56/1514.html >. Acesso em: 25 ago. 2017.
Graham Murdock, 2004. “Popular representation and postnormal science: The struggle over genetically modified foods,” In: Sandra Braman (editor). *Biotechnology and communication: The meta–technologies of information*. Mahwah, N.J.: Lawrence Erlbaum Associates, pp. 227–260.	MURDOCK, Graham. Popular representation and postnormal science: the struggle over genetically modified foods. In: BRAMAN, Sandra (Ed.). **Biotechnology and communication**: the meta–technologies of information. Mahwah, N.J.: Lawrence Erlbaum Associates, 2004, p. 227–260.
Bonnie A. Nardi and Vicki L. O’Day, 1999. “Information ecologies: Using technology with heart,” *First Monday*, volume 4, number 5 (May), at http://www.firstmonday.org/issues /issue4_5/nardi_contents.html, accessed 9 August 2006.	NARDI, Bonnie A.; O’DAY ,Vicki L. Information ecologies: using technology with heart. **First Monday**, v.4, n. 5, May 1999. Disponível em: <http://www.firstmonday.org/issues /issue4_5/nardi_contents.html>. Acesso em: 9 Aug. 2006.
Helen Nissenbaum, 2004. “Privacy as contextual integrity,” *Washington Law Review*, volume 79, pp. 119–157.	NISSENBAUM, Helen. Privacy as contextual integrity. **Washington Law Review,** v. 79, p. 119–157, 2004.
Richard A. Posner, 2002. *The problematics of moral and legal theory*. Cambridge, Mass.: Harvard University Press.	POSNER, Richard A. **The problematics of moral and legal theory**. Cambridge, Mass.: Harvard University Press, 2002.
Douglas L. Rogers, 2003. “The SCO litigation: Maintaining walls around trade secrets or attacking the knowledge of those outside the walls?” *Intellectual Property & Technology Law Journal*, volume 15, pp. 1–15.	ROGERS, Douglas L. The SCO litigation: maintaining walls around trade secrets or attacking the knowledge of those outside the walls? **Intellectual Property & Technology Law Journal**, v. 15, p 1–15, 2003.
Jennifer L. Saulino, 2002. “Locating inevitable disclosure’s place in trade secret analysis,” *Michigan Law Review*, 2002 (March): pp. 1184–1214.	SAULINO, Jennifer L. Locating inevitable disclosure’s place in trade secret analysis. **Michigan Law Review**, v. 100, n. 5, p. 1184–1214, Mach 2002. Disponível em: <https://www.jstor.org/stable/1290506?seq=1#pa

	ge_scan_tab_contents >. Acesso em: 25 ago. 2017.
Christina Schwenkel, 2006. “Recombinant history: Transnational practices of memory and knowledge production in contemporary Vietnam,” *Cultural Anthropology*, volume 21, number 1, pp. 3–30.	SCHWENKEL, Christina. Recombinant history: transnational practices of memory and knowledge production in contemporary Vietnam**. Cultural Anthropology**, v. 21, n. 1, p 3–30, 2006. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1525/can.2006.21.1.3/abstract >. Acesso em: 25 ago. 2017.
SCO v. IBM, case #2:03cv00294 DAK in the U.S. District Court Central Division, District of Utah (trial scheduled for 2007).	SCO. Caso SCO versus IBM, Caso #2:03cv00294 DAK in the U.S. District Court Central Division, District of Utah (trial scheduled for 2007).
Harriet J. Sims, 1977. “Recent Developments,” *George Washington Law Journal*, volume 65, p. 1641.	SIMS, Harriet J. Recent developments. **George Washington Law Journal**, v. 65, p. 1641, 1977.
Robert David Steele, 1990. “Intelligence in the 1990’s: Recasting national security in a changing world,” *American Intelligence Journal*, volume 11, number 3, pp. 29–36.	STEELE, Robert David. Intelligence in the 1990’s: recasting national security in a changing world. **American Intelligence Journal**, v.11, n. 3, p. 29–36, 1990.
Lee S. Strickland, 2005. *Secure information sharing: Balancing classification policies in an electronic era with new adversaries*. College Park: Center for Information Policy, University of Maryland; prepared for the Information Security Oversight Office, National Archives and Record Administration, at http://www.cip.umd.edu/reports/ISOO_report_final.pdf, accessed 9 August 2006.	STRICKLAND, Lee S. **Secure information sharing**: balancing classification policies in an electronic era with new adversaries. Maryland: College Park/ Center for Information Policy, University of Maryland, 2005. (Prepared for the Information Security Oversight Office, National Archives and Record Administration). Disponível em: <http://www.cip.umd.edu/reports/ISOO_report_final.pdf> . Acesso em: 09 Aug. 2006.
Cass R. Sunstein, 1996. *Legal reasoning and political conflict*. New York: Oxford University Press.	SUNSTEIN, Cass R. **Legal reasoning and political conflict.** New York: Oxford University Press, 1996.
Donald F. Theall, 1999. “The carnivalesque, the Internet and control of content: Satirizing knowledge, power and control,” *Continuum: Journal of Media & Cultural Studies*, volume 13, number 2, pp. 153–164.	Theall, Donald F. The carnivalesque, the Internet and control of content: satirizing knowledge, power and control. **Continuum: Journal of Media & Cultural Studies**, v.13, n. 2, p. 153–164, 1999.
Martin L. Van Creveld, 1991. *Technology and war: From 2000 BC to the present*. Revised and expanded edition. New York: Free Press.	VAN CREVELD, Martin L. **Technology and war:** from 2000 BC to the present. Rev. e ampl. New York: Free Press, 1991.
Lloyd L. Weinreb, 2005. *Legal reason: The use of analogy in legal argument*. Cambridge: Cambridge University Press.	WEINREB, Lloyd L. **Legal reason**: the use of analogy in legal argument. Cambridge: Cambridge University Press, 2005.