Chapter 27
Controlling Informational Society:
A Google Error Analysis!

Gonçalo Jorge Morais da Costa
De Montfort University, UK

Nuno Sotero Alves da Silva
De Montfort University, UK

Piotr Pawlak
Adam Mickiewicz University of Poznan, Poland

ABSTRACT

"Informational Society" is unceasingly discussed by all societies' quadrants. Nevertheless, in spite of illustrating the most recent progress of western societies the complexity to characterize it is well-known. In this societal evolution the "leading role" goes to information, as a polymorphic phenomenon and a polysemantic concept. Given such claim and the need for a multidimensional approach, the overall amount of information available online has reached an unparalleled level, and consequently search engines become exceptionally important. Search engines main stream literature has been debating the following perspectives: technology, user level of expertise and confidence, organizational impact, and just recently power issues. However, the trade-off between informational fluxes versus control has been disregarded. So, our intention is to discuss such gap, and for that, the overall structure of the chapter is: information, search engines, control and its dimensions, and exploit Google as a case study.

INTRODUCTION

The term "Information Society" or "Informational Society" emerges continuously in contemporary discussion. The intricacy to define it is well-known, but simultaneously, its content is somewhat clarified, when investigating the key features that characterize the most recent evolutional stage of western societies: communication, interaction, automation, post-industrial, specialist, service, immaterial needs, postmodern, or learning society (Castells, 2000; Webster, 2006). However, Ives Courrier (2000) differentiates "Information society", and "Knowledge society". Nevertheless, the historical roots of this sociological debate lie on the

DOI: 10.4018/978-1-61520-975-0.ch027

work of Fritz Machlup (1962) and Peter Drucker (1969) to describe the changing economical paradigm. This work has been incessantly updated in order to demonstrate the economical, sociological, or even philosophical reconfigurations.

Given the introductory analysis an important question arises: how can "Information Society" or "Informational Society" be defined or characterized? During the World Summit on the Information Society in 2003, representatives of governments and civil society organizations from 175 countries declared that: "… common desire and commitment to build a people-centred, inclusive and development oriented Information Society, where everyone can create, access, utilize, and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life" (World Summit on the Information Society, 2003, pp. 1). Plus, the European Commission describes it as: "the society currently being put into place, where low-cost information and data storage and transmission technologies are in general use. This generalization of information and data use is being accompanied by organizational, commercial, social and legal innovations that will profoundly change life both in the world of work and in society generally" (European Commission, 1997, pp. 15).

Therefore, it is understandable that governments or organizations, want to make sure that they are not left out of the opportunities associated with the information society (Lallana, 2004). However, before governments or organizations proceed to developing plans and strategies for the information society, it is important to investigate the underlying key feature of this paradigm: information. Information taxonomies are intrinsically bounded to the level of abstraction adopted, gather of requirements and desiderata orientating a theory (Shannon, 1948; Butler, 2001; Floridi, 2003; Kornai, 2008). As a consequence of computer networks the available information increased exponentially, allowing that search engines become remarkably important.

A search engine is a program that sends a spider to "crawl" web pages, in order to extract links, and in return the information found on the page (Pinkerton, 1994). So far, search engines literature focuses its attention on the following perspectives: technology (Zien et al., 2006), user level of expertise and confidence (Teevan, Dumais & Horvitz, 2005), organizational impact (Wielki, 2008), and just recently power issues (Rieder, 2005).

However, the ethical impacts concerning informational fluxes versus control have been disregarded. In order to obtain a plausible answer concerning this theoretical gap, it is crucial to address control and its boundaries. Therefore, it is vital to perceive what technological means allow to control and monitor cyberspace (Glorioso, 2008), as well as, what ethical and legal dilemmas arise to society in case of overstated control (Jung, 2001). As a final remark, the authors will include Google as case study due to its remarkable excellence recognized through its market share, but also as a consequence of their personal experience using search engines, namely this.

BACKGROUND

Information

Etymologically information derives from "inform", which means "to give form to, put into form or shape" (Oxford English Dictionary, 2008). In fact, the earliest characterizing example of this concept in accordance to the Oxford English Dictionary arises in 1590, when Edmund Spense wrote in *The Faerie Queene* about "infinite shapes of creatures…informed in the mud". However, the ancient Greek word *εἶδος* ("eidos") denoted the ideal identity or essence of something in Plato's philosophy. So, metaphorically "information"

represents not only a communication, but also a belief or a decision. Therefore, it is possible to describe information as a polymorphic phenomenon and a polysemantic concept so, as an *explicandum*, which can be clarified by some research disciplines, depending on the level of abstraction adopted, cluster of requirements and desiderata orientating a theory.

Given the nature of our argument, information will be approached by the following perceptions: mathematical, economical, biological, semantical, philosophical and ethical.

The complete absence of semantically content is bounded to Claude Shannon's theory (1948), in which information is related to uncertainty. Following Martin (1995), Shannon attempts to see information as a "thing" leading to a tangible analysis when compared to knowledge, which is rather intangible by nature (Rowley, 1998). Therefore, this tangible dimension of information implies a natural conclusion: information can be seen as a "commodity". According to Cash, MacFarlan & McKenney (1992), information can be seen as a raw material that will be used by a manufacture in the following production stage. This analogy illustrates the idea that information can be considerably different in accordance to its function or future function into the economical process.

Nevertheless, several authors illustrate information qualities as an economical resource (Jarvenpaa & Staples, 2001):

- **expandable:** because it increases with use;
- **compressible:** allowing to be summarized;
- **substitute:** information can substitute other resources;
- **transportable:** it is virtually instantaneous;
- **diffusive:** tending to leak from the straightjacket of secrecy and control, and the more it leaks the more there is; information is sharable, not exchangeable;
- **human:** it exists only through human perception.

For the biological consideration we plead Lange & Lapp (2007), nevertheless the work of Jonas Salk & Jonathan Salk (1981) is considered praxis. These authors defined three main eras of the universal evolution and increasing complexity. They outline three types of systems (or matter): physical, biological, being each of them characterised by new emergent and essential properties. The emergence of a new third system properly narrowly incident to new aspects (or types) of information, because in higher levels are important aspects of information from lower levels of physical systems (intrinsic property of systems).

Finally, the other three dimensions- semantical, philosophical and ethical- are intrinsically correlated with the metaphor of a precious fluid (Lakoff & Johnson, 1980). These authors related the features of ordinary liquids like water and to less tangible but nevertheless appealing notions like *chi*. Information can flow from a source to a recipient over a channel and it can be diluted, compressed, or stored in vessels of specific capacity, using a fluid metaphor to express it. Classical information theory provides a rational reconstruction of the fluid metaphor, with the bit as the fundamental volumetric unit from which other units such as channel capacity are derived by standard dimensional analysis. These informational fluids go far beyond mathematical representations, requiring a semantic analysis (Himma, 2005) or, philosophical (Floridi, 2005). Through the combination of these analyses Kornai (2008) illustrates that information as fluid engages the following characteristics: identity, sentience, volition, and reverence.

Search Engines

The exponential growth of informational fluxes in the digital age, lead to a critical issue: information retrieval. Web search is today one of the most challenging problems of the Internet, striving at providing users with the most relevant search results to their information needs (Finkelstein

et al., 2002). The instrumental tool that allows such achievement is a search engine, which can be described as a database that defines the set of documents that can be searched by the search engine (Wang, Meng & Yu, 2000). Or, it is a two-directional gateway: from the information provider to the user and from the user to the information provider. A search engine determines which information provided by information provider can be found by the end-user, as well as, what information the end-user will ultimately find (Liddy, 2003). Moreover, search engines can be classified as general or specialized. Specialized search engines index data from a specific domain, as opposed to general search engines, which attempt to index a broad range of information (Min, 2004).

According to Introna & Nissenbaum (2000), only in United States in 2000 Internet users conducted 6.9 billion searches! This importance has been a subject of research (see Hoffman & Novak, 1998); however, only recently power issues have been addressed (Elseem, 2007).

Nevertheless, main stream literature seems only to perceive the following analytical dimensions:

- **search engine evaluation**: this taxonomy induces multiple criteria, as for instance evaluation using click through data, and a user model (Dupret, Murdock & Piwowarski, 2007). Wang & DeWitt (2004) debate computing page rank in a distributed Internet search system. Lakshminarayana (2009) investigates how search engines categorize web pages. Or, finally, if the search engine brand name influences search results (Bailey, Thomas & Hawking, 2007);
- **website indexing versus queries results:** a research conducted by Ding & Marchionini (1996), first pointed a small overlap between results retrieved by different Web search engines for the same queries. However, Lawrence & Giles (1998) have demonstrated that a search engines indexes no more than 16% of all Websites. In accordance to Search Engine Watch (2005), this is a result of millions of new pages are added every single day. Plus, web query characteristics may influence these results (Zien, Meyer & Tomlin, 2001);
- **queries taxonomies**: Broder (2002) developed a web search taxonomy that classifies the ''need behind the query'' into three classes: navigational, informational, and transactional. Navigational are tasks where the user's intent is to find a particular web page. Informational arise when the purpose is to find information about a topic that may reside on one or more web pages. Transactional search tasks reflect the desire of the user to perform an action. Moreover, Kang and Kim (2004) demonstrated that optimizing search engines based on implicit data about informational versus navigational search improved performance;
- **information retrieval**: focuses how users retrieve online information and assimilate it even across more diverse niches (Evans & Card, 2008), allowing to understand what web aids are necessary. Literature still engages the analysis of intelligent information seek (Perkowitz & Etzioni, 2000; Domingues et al., 2008) and ontology design based on the schemas of databases and collection of queries that encompasses users areas of interest (Kashyap, 1999);
- **linguistic possibilities**: search engines have evolved, however the use of non-western language characters is still a limitation. Therefore, some studies are trying to evaluate how a search engine deals with these characters (Sornlertlamvanich, Tongchim & Isahara, 2007);
- **cached content**: evaluate the existing cached content in search engines has been a growing concerning by societies, there-

fore some studies have been conducted regarding such subject (see for example: Anagnostopoulos, 2007);

- **sponsored search**: a whole new range of issues has evolved due to the use of sponsored search (Fain & Pedersen, 2006). For example, Jansen & Mullen (2008) provide an overview of the factors that have led to the development of these sponsored web search platforms;
- **user's profiling**: Teevan, Dumais & Horvitz (2005) point out the value of personalizing web search. Other studies attempt to determine the user's intent of using a web search engine (Jansen, Booth & Spink, 2007), or user's behaviour regarding their information need or formulating their queries (Machill et al., 2003), as well as a refined ontology for the informational needs of the users community, which is targeted (Kashyap, 1999). Moreover, Shen, Tan & Zhai (2006) exploit the relationship between personal search history and accuracy, which can be perceived as Internet search strategy (Ruvini, 2003). Finally, Agichtei et al. (2006) strive to predict web search results through learning user interaction models;
- **organizational impact:** similarly to the power and legal issues only recent become a topic under discussion (Wielki, 2008).

In conclusion, search engines are a vital tool regarding informational fluxes. Still, an ethical debate concerning related to control, transparency and legal issues has been neglected.

Informational Fluxes vs. Security

Information security is scarcely a novel conception, as well as the need to protect information, given how this concept forged mankind evolution. However, the "Information Society" translates a critical stage of protection concerning four key elements of informational flows (Bossi et al., 2004): availability, integrity, authenticity, confidentiality. While the idea of information security is certainly not new, the practice of information security has been and continues to be an evolving endeavour where in technological advances both help and hinder its progress. The advent of the information age, as a messenger of rapid and widespread digital computing and networking technologies, has fundamentally changed the practices concerning informational fluxes, adding a new dynamic to computer security (Seehusen & Stolen, 2008).

In the networked world or cyberspace (combination of the World Wide Web, Deep Web and other networks) informational fluxes are instantaneous, leading to a whole new range of security (computer virus, hacking, etc.) and ethical issues (privacy, intellectual property, transparency, equity, etc), because data is easily copied, transmitted, modified or destroyed. In March 2009, Internet had 1.596 billion users (Miniwatts Marketing Group, 2009) accessing through multiple technological platforms, leading to an important conclusion: even a minute percentage of people with malicious intent, constitute a substantial threat.

In 2002, the Organization for Economic Co-operation and Development (OECD) released the document *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (Organization for Economic Cooperation and Development, 2002), with the intention to initiate a new international acceptance concerning information systems safeguard. In spite of this effort the drawbacks detected by Cuppens (2001) seem to continue (see Ganame et al., 2008); however, we need to recognize the effort of evolving technologies in order to minimize these risks. Therefore, the following step of our analysis is to debate the current available technologies that allow informational entities to preserve their informational fluxes, which can be categorized into:

- **human filtering**: our bodies will be the keys that give us access to the Internet (Bullinga, 2001);
- **machine filtering**: embraces hardware and software technological regarding informational fluxes and content (Patterson, Shepherd & Watters, 2000).

Biometrics is the use of technology to recognise individual human features such as fingerprints, retinas and hand prints. That is, a computer can be programmed to identify an individual by recognising each individual's thumbprint (Crowley, 2006). Such technology needs not only to protect the stored personal data that underpin biometric authentication, but also the biometric image that is unique to each individual. Enhanced protection can be gained by use of a mixture of security techniques.

The leading providers of informational fluxes, as for example Internet Service Providers (ISP's) or search engines, have at their disposal firewalls, anti-virus, and anti-spyware grids that allow to describe the behaviour of current viruses, spyware or other bad code which is circulating (Microsoft Corporation, 2009; Heise, 2009), establishing an appropriate securing mechanism through a security policy (Federal Office for Information Security in Germany, 2008).

Regarding content based filtering, *deep pack inspection technologies*, allowed a more effective analysis concerning data that is intercepted and analyzed (Glorioso, 2008). However the effectiveness of content filters is still discussable (Thornburgh & Lin, 2002), given two kinds of errors: blocking a page that should not be blocked, *overblocking*; and, failing to block a page that should be blocked, *underblocking* (Stark, 2007). Finally, the core technologies that allow content filtering are (Patterson, Shepherd & Watters, 2000):

- **site labels**: labelling refer to schemes to assign content related labels to Uniform Resources Locator (URL's) and/or specific Web pages. Once a label schema has been chosen by a service or a community, then a Platform for Internet Content Selection (PICS) is required to implement that schema for individual Web pages;
- **lists of appropriate or inappropriate sites**: most frequently used content control mechanism is the use of lists of acceptable and/or unacceptable URL's;
- **automated text analysis**: another way to analyze a Web site is to use software that scans the text of a site to determine the relevance or suitability of pages.

In conclusion, in spite of the positive evolution of these technologies it is urgent to understand, if they ethically comply with the admissible policy enforced by the automated system (Gan & Suel, 2007).

Information Control

Conceptualizing Control

Following the etymological roots of control, it is possible to acknowledge that is a "power" that directly determines a situation; a relation of constraint of one entity (thing or person or group) by another, or, the state that exists when one person or group has power over another (Online Etymological Dictionary, 2008).

The Perception of Security

In an explanatory meaning, security and its complement in diverse languages, reproduce the affairs between object (subject) and its environment. Nevertheless it is imperative that security is a normative, an emotionally loaded idea (Mesjasz, 2004). Any attempts to elaborate a complete definition of security are of course vain, given the broader and expanded meanings of such concept. In fact, typically security is categorized in:

- a traditional meaning- security as an attribute of state, absence of military conflict (Kaldor, 2007);
- a broader sense- referring directly to a phenomena occurring in international relations, or directly/indirectly caused by inter-state relations security as a public good (Buzan, 2003; Deudney, 2004);
- a universal sense (of a unit and of a social entity)- human security (Cahill & Melo, 2004; Nickel, 2007).

Moreover, considering an etymological discussion a double outlook appears: the Latin expression is *secures*, meaning safe or secure. Adding the noun *cura* (care), security becomes a quality or state of being secure, or as a freedom from danger. This is similar what Cycero claims: the absence of anxiety upon which the fulfilled life depends (Liotta, 2002). The following interpretation is bounded to the word *securus*, which initially referred to liberation from uneasiness, or a peaceful situation without any risks or threats. Nevertheless, the linguistic perception of security is often shaped by cultural elements leading to more interpretations (Morgenthau, 1960).

Given the nature of argument the authors will draw their attention to the universal sense of security. Our decision may seem awkward, namely given the United Nations (UN) (2008) report: the concept of security must change- from an exclusive stress on national security to a much greater stress on people's security, from security through armaments, human development, territorial security to food, employment and environmental security (United Nations, 2008); however, given the potential *Tragedy of Good Will* (Floridi, 2006) that computer networks configure (insecure or lack of integrity concerning personal data, absence of privacy, and other ethical issues), the argument seems perfectly justifiable. Plus, the authors plead the argument of Manunta (2000) that security in a philosophical sense entails into the sense of freedom due to perception, or awareness of not existent "worries" or "dangerous", which computer networks seem to promote in user's, in spite of *Barbarians at the Gate* (Mierzejewska, 2008). Therefore, this "unintended ignorance" may provoke serious consequences!

Informational Fluxes vs. Control

Searching on the Web expands from a quick question to "progressive or composite", for which a lot of information is known to exist. Casual users simply cause a quick question; and, "usual" users understand the need for query syntax or, search engine construction features and operations, according to their potential interests and curiosity (Decker, 2008). Plus through the work of Pirolli & Card (1999), is possible to comprehend how user strategies and technologies for information seeking, gathering, and consumption interact concerning the environmental fluxes of information, leading to the following concepts as Furnas (1997) pleads:

- **information scent**: imperfect information at intermediary locations that is applied by the searcher to decide what paths should take in order to target information through a library or an on-line text database;
- **information diet**: information distributed by link descriptors, images, contextual clues, such as preceding headings, or by page arrangement.

Therefore, search engines try to provide users the information that satisfies their needs, however with the growing number of pages created every day their information retrieval process versus control become relevant. An example of this dilemma is illustrated in project WebWatcher, which encompasses an information agent that is tries interactively to deliver what information is sought. In fact, as the user navigates through the Web, the software utilizes its learned knowledge to recommend especially promising hyperlinks to

the user by highlighting these links on the user's display (Armstrong et al., 1995).

Nonetheless, the level of exposure of search engines to possible malicious attacks, or other intended practices or content is extremely high (Fishkin & Pollard, 2007; Schlembach, 2008). These authors have demonstrated through studies that usually Hypertext Preprocessor (PHP) pages (responsible for delivering search results) are compromised in certain keywords due to malware; or, proxy abuses that are typical of rogue search engines. In that sense, metaphorically the authors address the work of Cao, Feito & Touchette (2009) regarding stochastically informational fluxes control, who claims that control theories have two types of ratchets: open-loop, and closed looped. The first group concerns the appliance of a rectifying potential independently state of the system to be controlled; and the second engages a rectification action on a system has an explicit dependence on that system's evolution in time. Moreover, Decker (2008) claims the search engines optimization tools are based on two key factors:

- **on-site**: refers to contents and formats applied within the websites;
- **off-site**: engages the mainly associated URL's concerning to their domain reputation/ranking value.

Due to previous arguments the level of invisible Web[1], high-quality information, is not available due to search engines technical limitations, or will not, due to deliberate choice add to their indices of Web pages (Sherman and Price, 2001). Therefore, invisibility is a dynamic attribute that search engines must acquire, or else, some serious controversies will arise from search engines (Gerhart, 2004): often articulate the richness and intensity of a topic; dramatize change*;* may induce a critical dissimilarity in life by shifting decisions; scientists, journalists, and intelligence analysts are professionally mandatory to deal with multiple perceptions, evidences, authorities, and judgments on topics. In that sense, the authors agree with the arguments of Poullet (2009) concerning the two major trends that information society will face: the privatisation of cyberspace and, the global consequences of local actions and decision (for more details see section future trends).

A Organizational Approach

Human organizations are complex systems, which according to Kaufman (1995) are an organizational unit that it intends to preserve his identity and integrity, in order to guarantee its survival, being "forced" to interpret an amount of information greater than is processing capacity. Therefore, information security is an issue of tremendous concern to businesses worldwide (Whitman 2003), leading to a positive network externality (Kunreuther & Heal, 2002).

The management of information security should occur within all organizational levels (Gordon & Loeb, 2006), that is, expenditures for enterprise security have been distributed over tools, policies, technology, procedures and personnel to achieve the highest level of asset protection (Eloff & von Solms, 2000). However, top management has a different perspective and must answer the following question: what is the optimal enterprise-wide security budget that minimizes informational losses? So, "information" is an asset similar to other business assets.

The answer to this question establishes the budgetary boundaries for building a security capability and for acceptable losses, given the risk tolerances of decision makers (risk assessment analysis) (Anderson & Shain, 1991).

It involves modelling the costs of achieving various levels of best practice implementation in the presence of uncertain losses and establishes the optimal enterprise security budget using various decision criteria. The strategic management of security focuses on the competing demands for enterprise resources and their opportunity costs,

and seeks to identify security benefits that justify related costs (Kwon et al., 2007). If there were no threats, security resources would not exist, costs would be lower, profits higher, and entities would have higher equity values.

According to Turban et al. (1996), risk is the likelihood that a threat materializes. Risk is to some degree unavoidable, so the organization must accept some degree of risk. Therefore, the attitudes and tolerances for risks are considerably different given context, individual decision maker, and degree of uncertainty (Finne, 2000), leading to a gap between managers and technicians (Bakari et al., 2007). They also can vary with the absolute magnitude of probable and expected (average) losses, or the chosen risk analytical method (Gordon et al., 2006).

A Societal Approach

The Internet was born in the aftermath of technological advancement, which was fundamental to the US defence system. Thus, with its advent it was strictly administered by the American Defence Advanced Research Projects Agency (later DARPA). Formally speaking, in 1990 the US army yielded ground to the National Science Foundation. From this moment on, the truly global expansion of the Internet began and it went hand in hand with privatization. In 1991, in prospect of the impending deregulation of the Internet by the US administration, the National Science Foundation (NSF) established the Internet Society (ISOC), a watchdog of the future global Web development. Furthermore, the ISOC intended to prop up various groups of specialists working on the Internet advancement. American IT specialists- Vinton G. Cerf & Robert E. Kahn (TCP/IP protocol inventors), who are considered the Internet founding fathers, took the helm of the organization. However, as the Web was becoming more and more international, the institution's ambiguous status (which, although autonomous, was in fact controlled by the US administration) came into harsh criticism from governments from other countries, European ones in particular (Castells, 2001). Currently, the Internet Society is a US non-profit organization registered in the Washington city court with its branches scattered worldwide (in consequence, it is an international organization).

The Internet Corporation for Assigned Names and Numbers (ICANN) is yet another important organization, which shaped the Internet. For the purpose of a vast global representation, members of the Board come from various parts of the world. Yet, this perfect picture, where global Internet community appoints its representation by electronic ballot, is tarnished by lobbing of powerful groups and campaigns, which back up specific candidates. In the context of the prevalent influence of large corporations, a truly democratic operation in the ICANN formal structures is pure fiction. What is more, the organization is closely bound with the US Department of Commerce (Castells, 2001). As a result, the US is the main player in the ICANN, which from time to time is harshly criticized.

The World Wide Web Consortium (W3C) is another Web-shaping organization. It seeks to implement standard solutions in websites. The organization was established in 1994 by Tim Berners-Lee (WWW inventor). Its branches are scattered worldwide, but its headquarters are located in the US (with the Massachusetts Institute of Technology), in Europe, and in Japan. W3C currently affiliates over 500 organizations, companies, government agencies and universities from all parts of the world. The W3C publishes its recommendations, which however are not legally effective. Despite the fact, the organization is considered influential and must not be ignored. A company, or an organization, which wants to join the W3C "club" must pay annual membership fees, which are computed individually, depending on the candidate size (it seems logical to calculate higher fees for the more powerful members of the organization). The W3C members include orga-

nizations of various types, collages, universities, associations, companies of different size, among others, such giants as, for instance, Microsoft.

The discussion about the legal aspects of the Internet must touch upon the US IT security policy, as its regulations have exerted a tangible influence on the shape of the new medium. Indisputably, the US can be deemed a forerunner, when it comes to technological advancement, IT infrastructure, communication technology and connectivity. It can also be inferred that the US is the only country in the world with such a consistent and coherent IT security policy. It is largely based on cooperation between private and public entities. The idea stems from the American property structure. In the USA computer technology production is to a large extent private (Microsoft, IBM, HP, Compaq etc.) and the sector generates growing proceeds (Bogdat-Brzezinska & Gawrycki, 2003). For this world's top profitable business to operate safely, the company owners ensure that the high level security measures are applied. It is symbiotic, as it is a win-win situation for all parties involved.

The US ICT sector makes for a powerful lobby, which affects state policy in terms of government procurement, product licence protection. IT security policy constitutes a vital element of the entire national security policy. The US IT security is made up of legal acts, institutional regulations, political statements and numerous international activities, which, among others, seek to promote the global concept of cyber-defence (Bogdat-Brzezinska & Gawrycki, 2003) American technologies and democracy worldwide.

In the aftermath of the 9/11 attacks the US Congress adopted the "Patriot Act", which obliged Internet and ICT operators to monitor Web communication and provided federal services with access to private accounts and connections (therefore, the authorities are entitled to read e-mails, listen to and record telephone calls, etc.). On the premise that most of the Web operations "are transmitted" through systems located in the USA and that most of the Internet operators and suppliers are based there, it appears plausible for the US administration to control (or at least to have a capacity to control) the Internet communication. The USA is actively involved in numerous international undertakings pertaining to the widely understood ICT issues. It promotes the UN concept of information society and, for instance, provides ICT infrastructure assistance to APEC countries.

When it comes to the US international policy, it seeks to gain an edge and to be streets ahead of its competitors aspiring to the role of global technological leaders. In consequence, it implements initiatives, which undermine the role of the European Union and Japan in this field. Bill Clinton's and George Bush's (National Information Infrastructure) administration documents featured the concept of information society. It disseminates establishment of information highways as a part of national information web infrastructure, which makes the Internet widely available, but still chargeable. A closer look at the American strategy corroborates the statement that the concept of information society is to work for the benefit of business beneficiaries and to secure the US technological advantage in the world (Bogdat-Brzezinska & Gawrycki, 2003).

Many scholars perceive the Internet as a tool, which puts liberal ideas into practice (in particular, when it comes to communication). It is a common belief that the global Web (its architecture and operation) best safeguards observance of liberal rules, as there is no questioning the "freedom of speech" (the right to freely speak of one's opinions in public and to respect the opinions), "freedom of information" and "freedom of communication". Liberalism largely emphasizes individual liberty and values rights of an individual higher than the rights of a community. It promotes unlimited liberty of citizens to take actions (which are properly regulated, though) in all areas of collective life. There is no denying that the US still prevails in shaping the Internet and that the

US capital controls a substantial part of the ICT sector. In consequence of the prevalence, the American mainstream viewpoints are transposed on the ICT space. "American liberalism" (also referred to as "modern liberalism"), which is focal for this chapter, appears to be the chief and the most vital viewpoint of this type. In some aspects it differs from traditional liberalism. In contrast to classic liberalism, it promotes a more significant role of state both in social and business life. Hence, it seems that this ideology predetermines the premises of the security policy, which allows various business entities to oversee the widely understood information.

It is becoming increasingly common to state that freedoms of information and communication are more and more frequently regulated. The different forms of constraints and control are factor-dependent. They depend on the institutional organization of the Internet, government activities of various states and actions of various business entities. The first factor was elaborated on in the paragraphs above. When it comes to factor two, it is best illustrated by the US authorities' control of electronic media transported into the States. Laptops and mobile devices are browsed through and correspondence and documents stored on them checked. The Echelon system is also a good example. This world's leading signal intelligence collection and analysis network makes it possible to control 90% of digital information sent worldwide. The totality of business sector is subsumed under factor three. It is of significance, as it was noted by Castells in *The Internet Galaxy*. He concluded that business is one of four elements, which shape the Internet culture, but is the element, when it comes to Web content input.

The final factor is multi-aspect and complex. It covers a wide spectrum of corporate activities: with monitoring employees' conduct to begin with and Web consumer behaviour control, to end with. Particular electronic communication technologies are increasingly subject to control (for instance, by aggressive patent assignment). All these actions are taken as corporate security policy measures (understood as information security, including confidential information protection) and ICT security actions. Confidential information protection refers to information considered confidential by legal acts effective in a given country and information perceived trade secret by specific entities. The scope of protected (controlled) information can be wide and different depending on a given entity. Nonetheless, there is no doubt that in every case personal data must be protected and personal databases should be created and processed in a way which allows the identity and individuality be protected. Detailed information availability must be specified (to whom, where, when, to what extent, for what purpose). It is also a common obligation to promptly destroy outdated data as well as information, the processing purpose of which was attained.

The obligation to control information under the adopted security policy is in fact well-grounded. However, the regulatory structure, which serves as the basis for pertinent regulations, is too comprehensive and incoherent (Foucalt, 1986). As a result, there are (numerous) cases of abuses or actions, which verge on legitimacy and ethical rules. The corporate intention to control the largest possible scope of cyberspace information is in conflict with liberal freedom of information, which is the foundation of ICT revolution mechanism. The freedom is best characterized by Tim Berners-Lee (2000) about the World Wide Web service that he invented: if this technology was my property, was under my control, so probably would never have been invented. The decision to make the Web an open system was necessary to make it widely available. We cannot propose to make it a public space and still have it under our control.

FOCUS: THE CASE OF GOOGLE

Why Debate Google

The choice concerning Google is justifiable by its amazing evolution as a company, being recognized worldwide through its market share, but namely due its unique search engine. In spite of using a possible Google´s inaccuracy concerning user´s security or profiling, the truth is that Google is the best search engine available.

The idea of Google as a company emerged in 1995 when Larry Page and Sergey Brin started a project during the University. Given their difficult to find a buyer or receive funding, David Filo, the founder of Yahoo!, advised them to grow the service themselves (Information Week, 2008). For that, they had the assistance of their families and friends and, Andy Bechtolsheim as a business angel (Google, 2009a).

Near the year 2000 Google´s popularity was already considerable due to its unique organizational philosophies, to the introduction of new products (Google toolbar or AdWords) and a partnership with Yahoo. Giving their continuous innovation process regarding products (Addwords, Algorithmic Search, etc.), as well as, its business model (see for example, Google AdSense, Froogue, G-mail, Google Groups, Chrome, Maps, Wi-Fi services, etc.) Google become the worldwide market leader (Eisenmann & Herman, 2006; Lastowka, 2007), which is related with the company mission: "Google´s mission is to organize the word´s information and make it universally accessible and useful" (Google, 2009b); and name, "Googol" is the mathematical term for a 1 followed by 100 zeros (...)" (Google, 2009b).

This leadership is easily perceived through the evolution of the market share analysis regarding two dimensions: organic search, and paid search. Following Sisson (2004), this analysis entails into the following criteria:

- **number of indexed pages:** measures in billions the number of indexed pages, including types of files (Word, Excel, PDF, etc.) within a determined time period;
- **search-referral percentage:** computes the percentage of visitor traffic. This can comprise paid keywords, unpaid search results, and even banner ads on the search portal's web site within a determined time period;
- **number of performed searches:** determines in billion the number of conducted searches within a determined time period;
- **search time hours:** calculates in billion the number of conducted searches within a determined time period;
- **paid search accounts:** quantify in percentage the existent online advertising in the major online advertisers within a determined time period.

According to Lipsman (2003) scores for indexed web pages Google represented 32% of the market, Yahoo 25% and MSN 19%. Also considering WebSideStory (2004) collected data, the leader in on-demand Web analytics is Google with a search referral percentage of nearly 41 percent, up from 35.99 percent on 2003. Second place player and previous leading search referral domain, Yahoo, posted 27.40 percent, against the 30.95 percent on 2003. The third placed was MSN with 19.57 percent.

Plus, following Bausch & Han (2006) report *Mega View Search*, searches on Google and Yahoo grew 41 percent and 47 percent, respectively, outpacing the overall search growth rate of 36 percent. Google's searches increased from 2.1 billion in March 2005 to 2.9 billion in March 2006, while in the same time period Yahoo's searches increased from 907.8 million to 1.3 billion. The number three ranked search provider, MSN, reported a 9 percent year-over-year growth in searches, from 0.592 billion to 0.643 billion.

Finally concerning paid search market, Google appears to have a market share of 70 percent, fol-

lowed by Yahoo with a market share of 22 percent, and Microsoft with about 8 percent (SearchIgnite, 2008). However, including within the market other forms of online advertising would reduce Google's market share. Paid search accounts represents 41 percent of online advertising, but display advertising accounts for percent (Swisher, 2008). Google has only a 1.5 percentage share of display advertising. Display advertising, unlike paid search, is highly fragmented. Fox Interactive Media has the largest market share with 15.9 percent, followed by Yahoo with 10.5 percent, AOL with 5.8 percent, and finally Microsoft with 4.7 percent (Kawamoto, 2008).

This impressive growing has generated some critics and worries, namely under the analysis of US Anti-Trust Laws leading to the denial of Google and Yahoo agreement regarding advertising, because such partnership could represent around 70 to 80% of U.S. market share (see for example Lastowka, 2007; Hawker, 2008).

Google Search Engine

Google is well recognized, and it is possible that become even more widespread. The use of a search engine to detect information is vital, and traditionally, information search engine performance is measured along two dimensions: recall and precision. Recall is defined as the ratio involving the number of significant items retrieved and the overall amount of relevant items into the search space. Precision is acknowledged as the relation between the numeral relevant items retrieved and the total number of items (relevant and non-relevant) retrieved. In practice, there is an inverse correlation between recall and precision (Sullivan, 2002).

Google has tackled this challenge in a relatively unique way. Rather than pressing towards both perfect precision and recall, the engine's ranking technology, which uses link analysis to determine how important other sites on the Web deem a given item to be, enables Google to return quality results "early on." While this solution functions in many circumstances (and is most effective when the information sought for is general and popular), it still cannot fully answer the problem of relevance. Google works best as a mode of online research when one already has an understanding of the contextual features of a certain research domain. As Sisson (2004) claims in his metaphor: "The Google search engine is like a blind person reading a book in Braile- anything that is graphical, spatial, or visual in nature is simply not seen" (pp. 12). Moreover, this dilemma is still enhanced when the search topic list involves non-western languages, like Arabic or Hebrew. However, it is also necessary to recognize Google's in overcoming this dilemma (Physorg, 2006).

At this point however, some important questions arise: how Google really work? Which are its technical features that allow presenting the informational choice? Can locate an existing ontology, which conforms to the user's requirements?

After the users introduce the query, Google's webserver post it to the *index servers*. The content of these servers is comparable to an index, which refers which pages possess the corresponding words of the query. The following step of the process is to retrieve the documents from the *doc's server*, leading to the results delivery (Google, 2009c). All this process relies on *Google File System* (*GFS*), which consists of a single master and many chunk servers. Each file is broken into large chunks, identified with chunk handles. When a user intends to read or write a segment of a file, it calculates the chunk index using the offset of the segment and the size of a chunk (Ghemawat, Gobioff & Leung, 2003). The idea of *GFS* is to gain high performance and fault tolerant system using inexpensive hardware that often fails. *GFS* is optimized for storing large files, appending large amounts of data to the end of the file and making large streaming reads and small random reads. The system also features atomic concurrent appending of records into a single file with minimal synchronization overhead.

And the technical features? Checking the company's website once again, the authors conclude that Google's search engine gathers more than 200 signals in order to achieve which pages are more important. After that, a hypertext-matching analysis is conducted (Google, 2009c). However, not all the technical features are presented due to intellectual property issues, as recognized throughout our research. So, a detailed analysis of the technical features is required for: *PageRank*, *Bombs*, and *Hypertext-Matching Analysis*.

Google describes *PageRank* as the uniquely democratic nature of the web by using its vast link structure as an indicator of an individual page's value (Google, 2009c). In essence, Google interprets a link from page A to page B as a vote, by page A, for page B. But, Google looks at more than the sheer volume of votes, or links a page receives; it also analyzes the page that casts the vote. Votes cast by pages that are themselves "important" weigh more heavily and help to make other pages "important" (Huang & Paturi, 2005). These authors still point out some important drawbacks concerning this feature: spam abusing, evaluating older versus new pages, and spoofing. Spam problems are related to the possibility of an advertiser could have multiple spam pages pointing out for such destination page, leading to an enhancement of the *PageRank*. The second drawback concerns that older pages are tendentially more ranked. Finally, spoofing refers that *PageRank* would increase for all pages that vote for (or link to) a page.

Google's bombs acknowledge the intended practices of the company to manipulate the ranking of particular pages, in results returned by its search engine. The concept is related to the Internet jargon of improve a page ranking often due to humorous or political intentions (Zeller, 2006). However, Hiler (2002) proposed a broader typology of *Google's bombs*: fun, personal promotion, commercial, justice, ideological, and political. Nevertheless, Bar-Ilan (2007) debates each category illustrating several examples, and tries to determine if such examples are *Google's bombs*.

Hypertext-Matching Analysis refers how the search engine analyzes pages content. This feature represents a combination of text, fonts, location, and even neighbouring to determine the most relevant results (Google, 2009c). So far, literature did not recognize any drawbacks concerning Google's technology.

And what about the feature to locate an existing ontology, which conforms to the user's requirements? For Google the answer is "yes!", through its AdSense or Conceptual Information Retrieval and Communication Architecture (CIRCA), which is based on a language independent, scalable ontology consisting of millions of words along with what the words mean, how the words are related concept (Paulen, 2009), or even through Google Web API (Zhang, Vasconcelos & Sleeman, 2004). Moreover, as pointed out in DuCharme (2004), it is possible to simply use the Google facility "filetype:" to limit the type of searching file. At a first glimpse, Google presents suitable online ontology resources however, after some experiments (basically focused on finding RDFs files); the results are not the intended. Plus, it is very hard to use Google to search for suitable ontological files.

Google Security Features

In this section, the security measures undertaken by Google concerning privacy and data integrity, network security and its features, content policy will be detailed.

According to the company (Google, 2008a):

- it is not required to users give personal contact or demographic information;
- it never trades or crafts available individual names, lists of users, or aggregate data to any third parties;

- only uses client user configuration information to deliver;
- it maintains all user-specific and email message information, including content, addresses, categorizations, and IP addresses strictly confidential;
- it commits that client data will be protected following the provisions in its standard client contract:
- security and compliance products include specific confidentiality provisions in every client contract;
- when handling security and compliance products transactions, Google not just creates a contractual commitment but as well an operational in order to preserve client data integrity based on international standards;
- commitment concerning confidentiality and data security is integral to the security and compliance products' architecture.

Still in accordance to the company (Google, 2008a), the network security is achieved through duplicated storage systems and operational flows, with high degree of fault tolerance level. The operating system runs on a commercial version of Linux, however adapted and modified by Google. Nevertheless which are the features concerning network security, and measures taken? Google Search Appliance relies on a firewall as the main protection against malicious hackers (I-node, 2005); however, FitzGerald (2008) that is possible to inject spam into Google Web history. Plus, Nielson, Fogarty & Wallach (2004) point out that personal search engine contained serious security flaws that would allow a third party to read the search result summaries that are embedded in normal Google web searches by the local search engine. In spite of these critics McMillan (2006), acknowledges that through an agreement with Websense, Google detected over 2.000 malicious Web sites just in one month. Beyond the firewall, Delichatsios & Sonuyi (2005) resume the other measures: IP address recording and cookies.

Finally concerning content policy management, a deep content inspection using filters tries to enable security and regulatory violations to content. Policy options include the ability to block, quarantine, redirect, bounce, log, or even encrypt with *Google Message Encryption* (Google, 2008b). These filters combination is known as *Google's Giant Sandbox*, which started in March 2004. The sandbox filter appears to affect almost all new websites that were considered under the "probationer" category. In spite of appearing in the search results pages, if a website falls into such category it does not have immediate success (Daoust, 2009).

Reporting the Problem to Google

After debating Google's market share, its search engine, and its security features, it is time to introduce the key issue of our contribution. This matter is a consequence of Google long hour's usage, which can be bounded to the relationship between personal search history and accuracy (Shen, Tan & Zhai, 2006).

However, in order to allow a comprehensive recognition regarding the chapter focus, the authors will follow a four steps approach:

- **search question:** introduces an example concerning a possible search issue;
- **search process:** details how the search is conducted;
- **focus:** illustrates the input of our contribution;
- **reporting:** reports the communicational process between the authors and Google.

Consider a short search example concerning the debate of marketing and ethics. The following step is to perform the search; however previously to this, the strategy is to prepare a topic list with

different combinations to allow an improved outcome. Note that, the combination will be achieved through "search within results" within Google search engine. During the process the aim is to perceive the first 50 web pages that, Google give as a result for each search group. In spite of the speed reading rate for each web page be extremely fast, leading to a 5 minutes average time period for the 50 results, the aim is to download information for future reading.

After 30 minutes (average time), Google presents a web page stating the following message: "We're sorry... but your query looks similar to automated requests from a computer virus or spyware application. To protect our users, we can't process your request right now. We'll restore your access as quickly as possible, so try again soon in the meantime, if you suspect that your computer or network has been infected, you might want to run a virus checker or spyware remover to make sure that your systems are free of viruses and other spurious software. We apologize for the inconvenience, and hope we'll see you again on Google." Given this scenario the co-author is inhibited to continue his search at least for a 2 hours time period.

Plus, the following ideas must be pointed out:

- the personal computer of the co-author is protected against viruses or spyware;
- the co-author used several other protected personal computers, and even universities computer networks, which possess a higher level of security, and the outcome was equal.

After conducting a search within the company's website (including newsgroups and blogs) (Google, 2009d), the authors concluded that until now this issue have been not reported. Therefore, the communicational process started through an e-mail contact in November 24, 2008, in which the whole process and consequences were described (similar to this contribution). Google's answer was automatic acknowledging the e-mail acceptance, however imposing some conditions in order to continue the communicational process (see next section: Google's assumptions). Given no further contact by Google and with the problem still holding a phone call become a hypothesis! The main ideas of this contact are present also into the following section. Nevertheless, the key conclusion concerning it was that a similar e-mail should be submitted once again, which occurred in February 25, 2009. Until now, the feedback process engages the same results: Google's automatic response had recognized the e-mail, but no further contacts arise. Moreover, the characterized issue is still a reality!

Google's Assumptions

In order to comprehend Google's assumptions we need to approach three analytical dimensions, which are a combination of the communicational process (see previous section), and literature review:

- **search engines:** refers to the ethical dilemmas that search engine optimization imposes;
- **organizational:** acknowledges the ethical quandaries of organizational transparency;
- **reported issue:** the author's opinion concerning Google's perception of the reported issue and intended consequences.

The search engine optimization leads to ethical problems which usually are categorized into the main domains: the "white hats" that use "lawful" techniques to accomplish ranking; and, the "black hats" that employ more discussable practices (Hurlbert, 2004). According to Google Webmaster Guidelines (Google, 2006b) the concept "grey" defines the space between these domains, and follow the general rule-of-thumb of creating

pages for the users, not for the search engine. Plus, these guidelines outline that "black hats" methods need to be avoided. However, the key ethical dilemmas do not arise from this discussion, but from the search engine design characteristics (*PageRank*) and its intended consequences for users (stakeholders). Can a zero *PageRank* have real effects on the commerce of a website which is dependent on traffic from search engines? (United States District Court, 2006a; 2006b) Or, a zero *PageRank* configures the same results from a "search"? (Caufield, 2006) Moreover, the inexistence of a regulatory body of practices concerning ethical standards complied by all market players' results into the serious dilemmas, and enhances a pessimistic view of the "Information Society".

To address organizational transparency we will follow Vaccaro and Madsen (2006) to demonstrate the ethical and economical forces that affect a company organizational transparency. Engaging a top-bottom analysis Google's mission can lead to the first level of discussion: it will be possible? How Google will handle with the ethical dilemmas described by James Caufield. This author argues that search engines bear excessive ethical burdens given their influence in people's every day options. As "gatekeepers to information on the Web", companies like Google face two dilemmas: people's trust and, the socio-political implications that derive from have access not to a private space but to public, open and democratic properties (Caufield, 2006). These dilemmas are enhanced when the following questions are attended: can informational fluxes be controlled? And, who controls search engines?

Regarding Google's corporate information, it seems to disregard some underlying issues concerning information transparency, because is obsessive about his products characteristics and functioning, which is of course is a natural phenomenon; however, it is difficult to search or address other ways of working with its products even into corporate blogs. Moreover, in spite of technical questions are bounded to a specific technical service, which a very positive approach by Google and easily perceived in the corporate website; the truth is that for technical issues concerning the search engine does not exist any available contact, even performing a "search" within Google's help. Even, when contacting Google by phone the process is not transparent enough because who is contacting Google needs to know the person's name that you want to contact, or else the system gives as hypothesis the e-mails already presented in the website. So, in order to become a XXI century organization, transparency needs to bind to corporate values as a "mental state" (Costa, Prior and Rogerson, 2008).

For the reported issue our analysis will entail into two sub-dimensions: e-mails; and, phone call. Through the e-mails exchange it is possible to conclude that Google's assumes the importance of security issues, which is a positive sign; however, the automatic reply also claims that if a security problem was not being reported an answer will not be obtained, which had occurred. Moreover, during the phone contact two it was possible to understand that this issue is not related to security, and above all that until now this issue have been not reported by worldwide users.

Thus, an important question still remains: if it is not a security issue, then in what category it falls? Our personal believe given the previous arguments, and in some extent the critical work of Seth Finkelstein (2007), is that Google categorize it as a profiling issue. Profiling is a formal review or analysis of data, often in the form of a graph or table, representing distinctive features or characteristics of an object or a person's behaviour. Such process usually occurs through Technology Profile Inventory (TPI) (DeYoung & Spence, 2004), and it is possible to determine a hacker or spyware profile (Dantu et al., 2007). In this particular case, given the speed and the way search is conducted Google's assumes that the co-author has similar distinctive characteristics. As a consequence, productivity is seriously affect as well as equity, because an outlier's behaviour

or non traditional corresponding ways to conduct a search are also affected due to these controls. So, given the previous arguments some questions remained answered: which are the real economical costs concerning productivity losses? What criteria Google's TPI engages? It is fair to profile these outliers as spammers or viruses? It is possible to achieve a more flexible profiling? For example, why not engage a learning ontology (Li, Du & Wang, 2005) for the profiling system, allowing that users create queries involving them and their personal believes or experiences for information retrieval without be considered outliers, as well as reflects the true informational needs of the user community.

FUTURE TRENDS

Search engines evolution will never rest in order to increase the quality and relevancy of the results, as well as, to diminish *PageRank* limitations, spam and viruses (Achte, 2006). A lot has changed over the years, and the future is sure to also deliver its plethora of surprises, but this growing role leads to even greater ethical dilemmas. Thus, the question is how to control their actions trough legal acts, and since Web 2.0 is becoming embedded into business models (European Parliament, 2002), the problem is enhancing. In spite of existing regulation, search engines are still largely "lost in law" or represent a policy vacuum.

Grimmelmann (2007) illustrates four broad areas of law that need to intervene:

- **intellectual property:** to what extent might search engines and hyperlinks infringe copyright laws? Beyond private copying, to what extent should other traditional exceptions to copyright apply in the digital environment? How to ensure that authors and other right holders are able to obtain proper remuneration for the exploitation of their material?;
- **free speech:** to what extent might search engines through their features allows free speech according to human rights conventions? Or, if it is possible to manipulate content?;
- **antitrust:** does the law and jurisdiction regarding to Internet activities different from other markets?;
- **openness (transparency) of search algorithms:** beyond traditional information, what information should be provided to stakeholders in order to guarantee transparency?

In addition, van Eijk (2007) points out privacy as another intervention. In spite of recognize the bound between freedom of expression and privacy, this author goes beyond that claim and acknowledges the need for a principle concerning a minimum of personal data that should be stored and processed, as well as the reason why it has been collected. Some critics may arise due to the Resolution on Privacy Protection and Search Engines; however, policy vacuums are still a reality. Moreover, the authors of this contribution still emphasise corporate responsibility regarding the liability of search engines in order to prevent issues similar to the reported one, which go further beyond Achte (2006) perception, so a truth organizational transparency occur.

Given such arguments, van Eijk (2009) recently presented a possible converged regulatory model for search engines with the following characteristics:

- **market power:** potentially pertinent as a basis for decision making concerning market regulation through several non-discriminatory, transparent and objective criteria;
- **relevant legal issues:** include "cloud computing", which in spite of produce efficiency concerning business, entails an absolute lack of transparency regarding the location

of sensitive data. So, within the scope of good governance, risks must be clearly defined.

However, we follow Grimmelmann (2005) claim that is needed representatives from all groups, and not a single resolution. For that, the authors' proposal is to present a joint solution between World Trade Organization (WTO) and UN in order to obtain plausible results, and given the global influence of information. The framework should engage two fundamental dimensions:

- **research:** will investigate possible law limitations and policy vacuums;
- **operability:** will monitor law compliance of each search engine worldwide and by region.

Finally, the procedures for both dimensions follows UN operations by regions, however given cultural differences, as for example, Eurasia region should be divided into Europe and Asia. Besides that, Europe should so be separated into: Mediterranean Europe, Central Europe, Eastern Europe, and North European countries.

CONCLUSION

Google is undoubtedly the best search engine available in any technological platform (Schofield, 2006), which is recognized worldwide. In fact, the focus of this contribution is a consequence of the previous argument and co-authors personal usage due to its unique features. Nevertheless, Google's profiling is non flexible and needs to evolve in order to allow outliers with ethical behaviours too perform their searches without any problem. Thus, in spite of Google's argument that "democracy on the web works" (Google, 2006a), and that *PageRank* do not influence or manipulates search results, the truth is that the perception of organizational transparency is affected (O'Shea, 2003; Livingston, 2004).

Even if, we accept Zook (2005) case concerning Internet as the Schumpeterian power for "creative destruction", Google's search engine in some extent controls informational fluxes, imposing serious ethical and legal challenges. Moreover, such dilemmas are enhanced and become normative due to pervasive computing. Like Wellman (2001, pp. 2) stated, it is precisely when "technological changes get pervasive, familiar and boring that their impact on society is usually most felt" (2001, p. 2), namely network personalization. Therefore, a wide and multidisciplinary debate is necessary concerning search engines!

As a final remark, it is necessary to understand that locking down a network resumes a trade-off between flexibility and control. Wherever the line is draw, it is important to be aware that gray areas will exist. Plus, if users do not possess technical expertise, could undermine acceptable usage policies.

REFERENCES

Achte, S. V. (2006). *Future evolution of search.* Resource document. Internet Search Engine Database. Retrieved February 20, 2009, from http://www.isedb.com/db/articles/1559/1/Future-Evolution-of-Search-/Page1.html.

Agichtein, E., et al. (2006). Learning user interaction models for predicting web search result preferences. In *Proceedings of the 29th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval* (pp. 3-10). Seattle, WA, USA.

Anagnostopoulos, I. (2007). Monitoring the evolution of cached content in Google and MSN. In *Proceedings of the 2007 International Conference on the World Wide Web* (pp. 1179-1180). May 8-12, Banff, Alberta, Canada. Retrieved January 22, 2009, from http://www2007.org/posters/poster993.pdf

Anderson, A., & Shain, M. (1991). Risk management. In Caelli, W., Longley, D., & Shain, M. (Eds.), *Information Security Handbook* (pp. 75–127). New York: Stockton Press.

Armstrong, R., et al. (1995). WebWatcher: A learning apprentice for the World Wide Web. In *AAI Spring Symposium on Information Gathering from Heterogeneous, Distributed Environments* (pp. 6-12). California: Stanford University, United States.

Bailey, P., Thomas, P., & Hawking, D. (2007). Does brandname influence perceived search result quality? Yahoo! Google, and WebKumara. In *Proceedings of the 12th Australasian Document Computing Symposium.* Retrieved March 7, 2009, from http://es.csiro.au/pubs/bailey-thomas-hawking-adcs2007.pdf.

Bakari, J. K. (2007). Bridging the gap between general management and technicians- A case study on ICT security in a developing country. *Computers & Security*, *26*(1), 44–55. doi:10.1016/j.cose.2006.10.007

Bar-Ilan, J. (2007). Manipulating search engines algorithm: The case of Google. *Journal of Information. Communication & Ethics in Society*, *5*(2/3), 155–166. doi:10.1108/14779960710837623

Barry, B., & Weaver, O. (2003). *Regions and powers: The structure of international security*. Cambridge: Cambridge University Press.

Bausch, S., & Han, L. (2006). *Nielsen//Net Ratings announces December US search engine rankings*. Resource document. NetRatings, Inc. Retrieved February 28, 2009, from http://www.nielsen-online.com/pr/pr_079123.pdf.

Berneers-Lee, T. (2000). *Weaving the Web: The original design and ultimate destiny of the World Wide Web*. New York: Collins Business.

Bogdat-Brzezinska, A., & Gawrycki, M. F. (2003). *Cyberterroryzm i problemy bezpieczenstwa informacyjnego we wspoczesnym swiecie. Fundacja Studiów Międzynarodowych*. Warszawa: Oficyna Wydawnicza ASPRA-JR.

Bossi, A. (2004). Unwinding in information flow security. *Electronic Notes in Theoretical Computer Science*, *99*, 127–154. doi:10.1016/j.entcs.2004.02.006

Broder, A. Z. (2002). A taxonomy of Web search. *ACM SIGIR Forum, 36*(2), 3-10. Retrieved March 25, 2009, from http://www.sigir.org/forum/F2002/broder.pdf.

Bullinga, M. (2001). *In total self/control: Internet 2005-2010. Verschijningsjaar, Nederlands: Ten Hagen Stam Uitgevers*. Den Haag.

Butler, B. S. (2001). Membership size, communication activity and sustainability: A resource-based model of online social structures. *Information Systems Research*, *12*(4), 346–362. doi:10.1287/isre.12.4.346.9703

Cahill, K., & Mello, S. V. (2004). *Human security for all: A tribute to Sergio Vieira de Mello*. New York: Fordham University Press.

Cao, F. J., Feito, A., & Touchette, H. (2009). Information and flux in a feedback controlled Brownian ratchet. *Physica A*, *388*(1/2), 113–119. doi:10.1016/j.physa.2008.10.006

Cash, J. I., McFarlan, F. W., & McKenney, J. L. (1992). *Corporate information systems management- The issues facing senior executives* (3rd ed.). Homewood, Ill: Business One Irwin.

Castells, M. (2000). *The rise of the network society: The information age: economy, society and culture* (2nd ed., *Vol. 1*). Malden: Blackwell.

Castells, M. (2001). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford: Oxford University Press.

Caufield, J. (2006). The myth of automated meaning. *International Review of Information Ethics*, *5*, 48–62.

Costa, G., Prior, M., & Rogerson, S. (2008). Will the evolution of ICT ethics engage organizational transparency? In Vaccaro, A., Horta, H., & Madsen, P. (Eds.), *Transparency, Information and Communication Technology- Social Responsibility and Accountability in Business and Education* (pp. 31–50). Virginia: Softbound.

Courrier, Y. (2000). Société de l'information et technologies. Report. *United Nations Educational, Scientific and Cultural Organization*. Retrieved April 5, 2009, from http://www.unesco.org/webworld/points_of_views/courrier_1.shtml.

Crowley, M. G. (2006). Cyber crime and biometric authentication- The problem of privacy versus protection of business assets. In *Proceedings of the 4th Australian Information Security Management Conference ECU - School of Computer and Information Science.* Perth: Edith Cowan University. Retrieved March 3, 2009, from http://scissec.scis.ecu.edu.au/conferences2008/proceedings/2006/aism/Crowley%20-%20Cyber%20crime%20and%20biometric%20authentication%20the%20problem%20of%20privacy%20versus%20protection%20of%20business%20assets.pdf.

Cuppens, F. (2001). Managing alerts in a multi-intrusion detection environment. In *Proceedings of 17th Annual Computer Security Applications Conference* 2001 (pp. 22-31). New Orleans, LO, USA.

Dantu, R. (2007). Classification of attributes and behaviour in risk management using Bayesian networks. In [New Brunswick, NJ: IEEE.]. *Proceedings of Intelligence and Security Informatics*, *2007*, 71–74.

Daoust, M. (2009). *Google's Giant Sandbox.* Resource document. Netbiz. Retrieved March 17, 2009, from http://www.netzbiz.com/Pages.asp?PageName=GGS.

Decker, A. (2008). *Search engines- How trustworthy are they?* Resource document. Trend Micro Inc. Retrieved April 4, 2009, from http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/avar_how_trustworthy_are_search_engines.

Delichatsios, S. A., & Sonuyi, T. (2005). *Get to know Google… Because they know you.* Resource document. Massachusetts Institute of Technology. Retrieved April 7, 2009, from http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/google.pdf.

Deudney, D. (2004). Publius before Kant: Federal-Republican security and democratic peace. *European Journal of International Relations*, *10*(3), 315–356. doi:10.1177/1354066104045540

DeYoung, C. G., & Spence, I. (2004). Profiling information technology users: En route to dynamic personalization. *Computers in Human Behavior*, *20*(1), 55–65. doi:10.1016/S0747-5632(03)00045-1

Ding, W., & Marchionini, G. (1996). A comparative study of Web search service performance. In S. Hardin (Ed.), *Proceedings of the 59th Annual Meeting of the American Society for Information Science* (pp. 136-142). Medford, NJ: Information Today, Inc.

Domingues, M. A., et al. (2008). A platform to support web site adaptation and monitoring its effects: A case study. In P. Pu, D. Bridge, B. Mobasher & F. Ricci (Eds.), *Proceedings of the 2008 ACM Conference on Recommender Systems* (pp. 299-302). Lausanne: École Polytechnique Fédérale de Lausanne, Switzerland.

Drucker, P. F. (1969). *The age of discontinuity: Guidelines to our changing society*. London: Heinemann.

DuCharme, B. (2004). *Googling for XML*. Resource document. O'Reilly XML Web site. Retrieved April 8, 2009, from http://www.xml.com/pub/a/2004/02/11/googlexml.html.

Dupret, G. E., Murdock, V., & Piwowarski, B. (2007). Web search engine evaluation using click-through data and a user model. In *Proceeding of the Workshop on Query Log Analysis: Social and Technological Challenges (WWW '07)*. May 8, Alberta, Canada. Retrieved January 25, 2009, from http://www2007.org/workshops/paper_28.pdf.

Eisenmann, T. R., & Herman, K. (2006). *Google Inc.* Harvard: Harvard Business School Publishing.

Elgesem, D. (2008). Search engines and the problem of transparency. In Bynum, T. W., Murata, K., & Rogerson, S. (Eds.), *ETHICOMP 2007: Glocalisation- Bridging the Global Nature of Information and Communication Technology and the Local Nature of Human Beings* (pp. 150–157). Tokyo: Meiji University, Japan.

Eloff, M. M., & von Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. *Computers & Security*, *19*(3), 243–256. doi:10.1016/S0167-4048(00)88613-7

European Commission. (1997). Building the European information society for us all: Final policy report of the high-level group of experts. *Office for Official Publications of the European Community*. Resource document. Retrieved April 11, 2009, from http://meritbbs.unimaas.nl/publications/2-hleg.pdf.

European Parliament. (2002). *Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services.* Resource document. Europa. Retrieved March 14, 2009, from http://europa.eu/scadplus/leg/en/lvb/l24216a.htm.

Evans, B. M., & Card, S. K. (2008). Augmented information assimilation: Social and algorithmic web aids for the information long tail. In *Proceedings of the 26th Annual SIGCHI conference on Human Factors and Computing* (pp. 989-998). San Diego: University of California.

Fain, D. C., & Pedersen, J. O. (2006). Sponsored search: A brief history. *Bulletin of the American Society for Information Science and Technology*, *32*, 12–13. doi:10.1002/bult.1720320206

Federal Office for Information Security in Germany. (2008). *Secure information technology- for our society*. Resource document. Federal Office for Information Security in Germany. Retrieved on February 25, 2009, from http://www.bsi.bund.de/english/publications/annualreport/BSI_annual_report_2006-2007.pdf.

Finkelstein, L. (2002). Placing search in context: The concept revisited. *ACM Transactions on Information Systems*, *20*(1), 116–131. doi:10.1145/503104.503110

Finkelstein, S. (2007). *Google spam filtering gone bad.* Resource document. Retrieved April 7, 2009, from http://sethf.com/anticensorware/general/google-spam.php.

Finne, T. (2000). Information systems risk management: Key concepts and business processes. *Computers & Security*, *19*(3), 234–242. doi:10.1016/S0167-4048(00)88612-5

Fishkin, R., & Pollard, J. (2007). *Beginner's guide for search engine optimization*. Resource document. SEOMoz.Org. Retrieved April 5, 2009, from http://www.seomoz.org/article/beginners-guide-to-search-engine-optimization.

Fitzgerald, N. (2008). *Re: [Full-disclosure] Injecting spam into Google web history via I'm feeling lucky queries*. Resource document. Derkeiler. Retrieved April 5, 2009, from http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-04/msg00540.html.

Floridi, L. (2003). Information. In Floridi, L. (Ed.), *The Blackwell guide to the philosophy of computing and information* (pp. 40–61). Oxford, New York: Blackwell. doi:10.1111/b.9780631229193.2003.00006.x

Floridi, L. (2005). Semantic conceptions of information. Resource document. *Sanford Encyclopedia of Philosophy*. Retrieved April 5, 2009, from http://plato.stanford.edu/entries/information-semantic

Floridi, L. (2006). Information technologies and the tragedy of good will. *Ethics and Information Technology*, *8*(4), 253–262. doi:10.1007/s10676-006-9110-6

Foucault, M. (1986). *Power/Knowledge: Selected interviews and other writings 1972-1977*. Sussex: The Harvester Press Limited.

Furnas, G. W. (1997). Effective view navigation. In *Proceedings of the SIGCHI conference on Human Factors and Computing* (pp. 367-374). Atlanta: University of Georgia, United States.

Gan, Q., & Suel, T. (2007). Improving Web spam classifiers using link structure. In *AIRWeb '07: Proceedings of the 3rd Int. Workshop on Advers. Inf. Retrieval on the Web* (pp. 17-20). Banff, Alberta, Canada. Retrieved February 10, 2009, from http://airweb.cse.lehigh.edu/2007/papers/paper_124.pdf.

Ganame, A. K., Bourgeois, J., Bidou, R., & Spies, F. (2008). A global security architecture for intrusion detection on computer networks. *Computers & Security*, *27*, 30–47. doi:10.1016/j.cose.2008.03.004

Gerhart, S. L. (2004). Do web search engines suppress controversy? *First Monday, 9*(1). Retrieved April 2, 2009, from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1111/1031.

Ghemawat, S., Gobioff, H., & Leung, S. (2003). The Google file system. In *SOSP '03: Proceedings of the nineteenth ACM symposium on Operating systems principles* (pp. 29-43). New York: ACM Press.

Glorioso, A. (2008). Ethics on a chip? Some general remarks on DRM, Internet filtering and trusted computing. In T. W. Bynum, M. Calzarossa, I. Lotto & S. Rogerson (Eds.), ETHICOMP 2008: Living, Working and Learning Beyond Technology (pp. 287-297). Mantova: University of Pavia, Italy.

Google. (2006a). *Our philosophy.* Resource document. Google. Retrieved February 20, 2009, from http://www.google.com/intl/en/corporate/tenthings.html.

Google. (2006b). *Webmaster guidelines*. Resource document. Google. Retrieved April 4, 2009, from http://www.google.com/support/webmasters/bin/answer.py?answer=35769.

Google. (2008a). *Security backgrounder: for Google security and compliance products.* Resource document. Google. Retrieved April 5, 2009, from https://www.postini.com/legal/Security_Backgrounder2.pdf.

Google. (2008b). *Content policy management.* Resource document. Google. Retrieved March 17, 2009, from www.google.com/a/help/intl/nl/security/pdf/content_policy_management.pdf.

Google. (2009a). *Google milestones*. Resource document. Google. Retrieved February 23, 2009, from http://www.google.com/intl/en/corporate/history.html.

Google. (2009b). *Company overview.* Resource document. Google. Retrieved February 23, 2009, from http://www.google.com/corporate.

Google. (2009c). *Technology overview.* Resource document. Google. Retrieved February 22, 2009, from http://www.google.com/corporate/tech.html.

Google. (2009d). *Google blog*. Resource document. Google. Retrieved February 22, 2009, from http://googleblog.blogspot.com/.

Gordon, L. A., & Martin, P. L. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, *49*(1), 121–125. doi:10.1145/1107458.1107465

Grimmelmann, J. (2005). *Regulating search?* Resource document. Yale Law School. Retrieved March 14, 2009, from http://james.grimmelmann.net/presentations/2005-12-03-search-engines.pdf.

Grimmelmann, J. (2007). *The structure of search engine law.* Resource document. *University of Iowa College of Law*. Retrieved April 4, 2009, from http://works.bepress.com/cgi/viewcontent.cgi?article=1012&context=james_grimmelmann.

Hawker, N. (2008). *The proposed Google-Yahoo alliance: An anti-trust white paper.* Washington: The American Anti-Trust Institute.

Heise Security. (2009). *Heise Security.* Resource document. Heise. Retrieved February 2, 2009, from http://www.heise.de/security/

Himma, K. E. (2005). Information and intellectual property protection: Evaluating the claim that information should be free. Resource document. *Berkeley Center for Law and Technology*. Retrieved April 5, 2009, from http://repositories.cdlib.org/bclt/lts/12.

Hoffman, D. L., & Novak, T. P. (1998). Bridging the racial divide on the Internet. *Science*, *280*(5362), 390–391. doi:10.1126/science.280.5362.390

Huang, R., & Paturi, R. (2005). *Analysis of the benefits and drawbacks of the PageRank algorithm*. Resource document. University of California. Retrieved February 8, 2009, from http://www.cse.ucsd.edu/~paturi/cse91/Presents/rhuang.pdf.

Hurlbert, W. (2004). *SEO ethics: Which hat to wear.* Resource document. Search Optimization. Retrieved April 4, 2009, from http://www.seochat.com/c/a/Search-Engine-Optimization-Help/SEO-Ethics-Which-Hat-To-Wear/.

I-node. (2005). *Security of the Google search appliances.* Resource document. I-node. Retrieved April 7, 2009, from http://www.i-node.it/documenti/GSA-physical-security.pdf.

Information Week. (2008). *The case of universal search: White paper*. Resource document. Information Week. Retrieved February 14, 2009, from http://www.informationweek.com/whitepaper/Internet/Search/the-case-for-universal-searc-wp1227642995192;jsessionid=0BRM2105ZCVD2QSNDLPCKHSCJUNN2JVN?articleID=50500003.

Introna, L. D., & Nissenbaum, H. (2000). Shaping the Web: Why the politics of search engines matter. *The Information Society*, *16*(3), 169–186. doi:10.1080/01972240050133634

Janse, B. J., & Mullen, T. (2008). Sponsored search: An overview of the concept, history, and technology. *International Journal of Electronic Business*, *6*(2), 114–131. doi:10.1504/IJEB.2008.018068

Jansen, B. J., Booth, D. E., & Spink, A. (2007). Determining the user intent of Web search engine queries. *WWW 2007*. May 8-12, Banff, Alberta, Canada. Retrieved March 3, 2009, from http://www2007.org/posters/poster989.pdf.

Jarvenpaa, S. L., & Staples, D. S. (2001). The use of collaborative media for information sharing: An exploratory study of determinants. *The Journal of Strategic Information Systems*, *18*(1), 151–183.

Jung, B. (2001). *Media, communication and electronic business*. Warsaw: Difin Publishing.

Kaldor, M. (2007). *Human security: Reflections on globalization and intervention*. Cambridge: Polity Press.

Kang, I.-H., & Kim, G. C. (2004). Integration of multiple evidences based on a query type for web search. *Information Processing and Management: An International Journal*, *40*(3), 459–478. doi:10.1016/S0306-4573(03)00053-0

Kashyap, V. (1999). Design and creation of ontologies for environmental information retrieval. In *Proceedings of the 12th Workshop on Knowledge Acquisition, Modelling and Management*. Alberta, Ontario, Canada. Retrieved April 3, 2009 from http://eprints.kfupm.edu.sa/34189/1/34189.pdf.

Kaufman, P. (1995). *New trading systems and methods*. London: Wiley.

Kawamoto, D. (2008). *Study: Fox Interactive tops digital display ad market.* Cnet News. Retrieved April 5, 2009, from http://news.cnet.com/8301-1023_3-10026578-93.html.

Kornai, A. (2008). On the proper definition of information. In T. W. Bynum, M. Calzarossa, I. Lotto & S. Rogerson (Eds.), ETHICOMP 2008: Living, Working and Learning Beyond Technology (pp. 488-495). Mantua: University of Pavia, Italy.

Kunreuther, H. C., & Heal, G. M. (2003). Interdependent security. *Journal of Risk and Uncertainty*, *26*(2/3), 231–249. doi:10.1023/A:1024119208153

Kwon, S. (2007). Common defects in information security management system of Korean companies. *Journal of Systems and Software*, *80*(10), 1631–1638. doi:10.1016/j.jss.2007.01.015

Lakoff, G., & Johnson, M. (1980). *Metaphors we live by*. Chicago, IL: University of Chicago Press.

Lakshminarayana, S. (2009). Categorization of web pages- Performance enhancement to search engine. *Knowledge-Based Systems*, *22*(1), 100–104. doi:10.1016/j.knosys.2008.07.006

Lallana, E. C. (2004). *An overview of ICT policies and e-strategies of select Asian economies*. New Delhi: APDIP.

Lange, J., & Lappe, M. (2007). The role of spatial and temporal information in biological motion perception. *Advances in Cognitive Psychology*, *3*(4), 419–428. doi:10.2478/v10053-008-0006-3

Lastowka, G. (2007). *Google's law.* Working Paper. Rutgers University. Retrieved February 20, 2009, from http://works.bepress.com/lastowka/4.

Lawrence, S., & Giles, C. L. (1998). Searching the World Wide Web. *Science*, *280*, 98–100. doi:10.1126/science.280.5360.98

Li, M., Du, X. Y., & Wang, S. (2005). Learning ontology from relational database. In D. S. Yeung, Z.-Q. Liu, X.-Z. Wang & H. Yan (Eds.), *Proceedings of the 4th International Conference on Machine Learning and Cybernetics* (pp. 3410-3415). Guangzhou: University of Guangzhou, China.

Liddy, E. D. (2003). Automating & evaluating metadata generation. *The Eighth Search Engine Meeting*. April 7-8. Boston, Massachusetts, USA.

Liotta, P. H. (2002). Boomerang effect: The converegence of national and human security. *Security Dialogue*, *33*(4), 473–488. doi:10.1177/0967010602033004007

Lipsman, A. (2003). *ComScore Media Metrix launches breakthrough system to track actual consumer search queries*. Resource document. Retrieved February 2, 2009, from http://www.comscore.com/press/release.asp?id=325.

Livingston, B. (2004). *Google grumbles*. Resource document. eWeek. Retrieved February 17, 2009, from www.eweek.com/article2/0,4149,1530367,00.asp.

Machill, M., et al. (2003). Wegweiser im netz: Qualität und nutzung von Suchmaschinen. In M. Machill & C. Welp (Eds.), Wegweiser im Netz (pp. 13-490). Gütersloh: Bertelsmann Stiftung.

Machlup, F. (1962). *The production and distribution of knowledge in the United States*. Princeton: Princeton University Press.

Manunta, G. (2000). Defining security. [Cranfield: Cranfield Security Centre.]. *Diogenes*, 1.

Martin, W. J. (1995). *The global information society. Brookfield, VT*. Aldershot: Aslib Gower.

McMillan, R. (2006). *Google's binary search helps identify malware*. Resource document. PC World. Retrieved March 17, 2009, from http://www.pcworld.com/article/126371/googles_binary_search_helps_identify_malware.html.

Mesjasz, C. (2004). *Security as a property of social systems*. Resource document. ISA Convention. Retrieved February 25, 2009, from http://www.allacademic.com/meta/p72561_index.html.

Microsoft Security Home Page. (2009). Microsoft Security. Resource document. Microsoft. Retrieved February 20, 2009, from http://www.microsoft.com/security/default.mspx.

Mierzejewska, B. (2008). Barbarians at the gate. In Wunderlinch, W., & Schimd, B. (Eds.), *Die Zukunft der Gutenberg-Galaxis* (pp. 99–116). Bern, Stuttgart, Wien: Haupt Verlag.

Min, P. (2004). *A 3D model search engine*. PhD Thesis. Computer Science. *Princeton University*. Retrieved March 3, 2009, from http://www.cs.princeton.edu/~min/publications/min04.pdf.

Miniwatts Marketing Group. (2009). *Internet world stats*. Resource document. Miniwatts Marketing Group. Retrieved January 5, 2009, from http://www.internetworldstats.com/stats.htm.

Morgenthau, H. J. (1960). *Politics among nations. The struggle for power and peace*. New York: Alfred A. Knopf.

Nickel, J. W. (2007). *Making sense of human rights*. Malden, Massachusetts: Blackwell Publishers.

Nielson, S., Fogarty, S. J., & Wallach, D. S. (2004). *Attacks on local searching tools*. Technical report. Department of Computer Science. Rice University. Retrieved March 17, 2009, from http://seclab.cs.rice.edu/pubs/gdesktop-tr-dec04.pdf.

O'Shea, D. C. (2003). The bloom is off the Google. *Optical Engineering (Redondo Beach, Calif.)*, *42*(4), 894. doi:10.1117/1.1569244

Online Etymology Dictionary. (2001). *Content*. Resource document. Online Etymology Dictionary. Retrieved January 1, 2009, from http://www.etymonline.com/index.php?l=c&p=24.

Organization for Economic Co-operation and Development. (2002). *OECD guidelines for the security of information systems and networks: Towards a culture of security*. Resource document. Retrieved February 2, 2009, from http://www.oecd.org/document/42/0,2340, en_2649_34255_15582250_1_1_1_1,00.html.

Oxford Dictionary. (2008). *Oxford English dictionary*. Oxford: Oxford University Press.

Patterson, C., Shepherd, M., & Watters, C. (2000). An ethical framework: mechanisms for user-enabled choice and normative claims. *INFOETHICS 2000*. Resource document. United Nations Educational Scientific and Cultural Organization, Paris. Retrieved March 8, 2009, from http://webworld.unesco.org/infoethics2000/report_151100.html#conley.

Paulen. A. (2009). Google Adsense Ontology. Resource document. *Enzine*. Retrieved April 5, 2009, from http://ezinearticles.com/?Google-Adsense-Ontology&id=290598.

Perkowitz, M., & Etzioni, O. (2000). Towards adaptive websites: Conceptual framework and case study. *Computer Networks*, *31*(11), 1245–1258. doi:10.1016/S1389-1286(99)00017-1

Physor. (2006). *Google buys a new search algorithm.* Resource document. Retrieved February 7, 2009, from http://www.physorg.com/news63882927.html.

Pinkerton, B. (1994). *Finding what people want: Experiences with the webcrawler*. The Second International WWW Conference Chicago, USA, October 17-20. Retrieved April 11, 2009, from http://www.webir.org/resources/phd/pinkerton_2000.pdf.

Pirolli, P., & Crad, S. K. (1999). Information foraging. *Psychological Review*, *106*, 643–675. doi:10.1037/0033-295X.106.4.643

Poullet, I. (2009). Data protection legislation: What is at stake for our society and democracy? *Computer Law & Security Report*, *25*(3), 211–226. doi:10.1016/j.clsr.2009.03.008

Rieder, B. (2005). Networked control: Search engines and the symmetry of confidence. *International Review of Information Ethics*, *3*(1), 26–32.

Rouvini, J.-D. (2003). Adapting to the user's internet search strategy on small devices. In L. Johnson & E. Andre (Eds.). *International Conference on Intelligent User Interfaces 2003* (pp. 284-286). Miami, Florida, USA.

Rowley, J. (1998). What is information? *Information Services & Use*, *18*(4), 243–254.

Salk, J., & Salk, J. D. (1981). *World populations and human values*. New York: Harper & Row Publishers.

Schlembach, I. (2008). *Reputation stat antivirus-software, URL-filter und blacklisting*. Resource document. SearchSecurity.de. Retrieved April 1, 2009, from http://www.searchsecurity.de/themenbereiche/plattformsicherheit/client-security/articles/120503/.

Schofield, J. (2006). *How does Google envisage the future?* Resource document. The Guardian. Retrieved March 17, 2009, from http://media.guardian.co.uk/newmedia/story/0,1726289,00.html.

SearchIgnite. (2008). *Potential impact of Google-Yahoo! Partnership & cost to marketers.* Resource document. Retrieved February 22, 2009, from http://www.searchignite.com/si/cm/tracking/trackredirect.aspx?siclientid=76&redirecturl.

Seehusen, F., & Stolen, K. (2008). *A method for model driven information flow security.* Report. University of Oslo, Norway. Retrieved March 3, 2009, from http://folk.uio.no/fredrise/publications/4.report-seehusen.pdf.

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, *27*, 379–423, 623–656.

Shen, X., Tan, B., & Zhai, C. (2006). Exploiting personal search history to improve search accuracy. In *Proceedings of 2006 ACM Conference on Research and Development on Information Retrieval- Personal Information Management Workshop (PIM'2006)* (pp. 94-97). Retrieved March 2, 2009, from http://pim.ischool.washington.edu/pim06/files/shen-paper.pdf.

Sherman, C., & Price, G. (2001). *The invisible Web*. Medford, NJ: Information Today, Inc.

Sisson, D. (2004). *Google secrets: How to get a top 10 ranking on the most important search engine in the world*. Redmond, WA: Blue Moose Webworks, Inc.

Sornlertlamvanich, V. Tongchim, S., & Isahara, H. (2007). Evaluation of Web search engines with Thai queries. In *Proceedings of Workshop on NTCIR-6 and EVIA-1, NII, National Center of Sciences* (pp. 17-21). Tokyo: Japan.

Stark, P. B. (2007). The effectiveness of Internet content filters. *A Journal of Law and Policy for the Information Society, 2*(3), 943-979.

Sullivan, D. (2002). *Google tops in search hours ratings*. Resource document. Search Engine Watch. Retrieved February 21, 2009, from http://searchenginewatch.com/sereport/article.php/2164801.

Sullivan, D. (2005). *Search engine sizes.* Resource document. Search Engine Watch. Retrieved March 25, 2009, from http://searchenginewatch.com/2156481.

Swisher, K. (2008). *Microsoft's trojan horse (also Google's): Display advertising.* Resource document. All Things Digital. Retrieved February 22, 2009, from http://kara.allthingsd.com/20080716/microsofts-trojan-horse-also-googles.

Teevan, J., Dumais, S. T., & Horvitz, E. E. (2005). Personalizing search via automated analysis of interests and activites. In *Proceedings of 28th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval* (pp. 449-456). New York: ACM Press.

Teevan, J., Dumais, S. T., & Horvitz, E. (2005). Beyond the commons: Investigating the value of personalizing Web search. In *Proceedings of the Workshop on new Technologies for Personalized Information Access, part of the 10th International Conference on User Modelling (UM '05)* (pp. 84-92). Retrieved March 2, 2009, from http://research.microsoft.com/en-us/um/people/sdumais/pia2005-final.pdf.

Thornburgh, D., & Lin, H. S. (Eds.). (2002). *Youth, pornography and the Internet*. Washington, D.C.: National Academies Press.

Turban, E., McLean, E., & Wetherbe, J. (1996). *Information technology for management: Improving quality and productivity*. New York: John Wiley & Sons.

United Nations. (2008). Human development report 2007/2008. Report. *United Nations*. Retrieved January 5, 2009, from http://hdr.undp.org/en/media/HDR_20072008_EN_Complete.pdf.

United States District Court. (2006a). *Kinderstart.com LLC v. Google Inc. first amended complaint, C 06-2057 RS*. Resource document. United States District Court: Northern District of California. San Jose. Retrieved February 10, 2009, from http://docs.justia.com/cases/federal/district-courts/california/candce/5:2006cv02057/178063/3/0.pdf.

United States District Court. (2006b). *Kinderstart.com LLC v. Google Inc. judgement order, C 06-2057 JF (RS)*. Resource document. United States District Court: Northern District of California. San Jose Division. Retrieved February 10, 2009, from http://docs.justia.com/cases/federal/district-courts/california/candce/5:2006cv02057/178063/43/0.pdf.

Vaccaro, A., & Madsen, P. (2006). Firm information transparency: ethical questions into the information age. In Berleur, J., Numinen, M. I., & Impagliazzo, J. (Eds.), *Social Informatics: An Information Society for All? In Remembrance of Rob Kling* (pp. 145–156). Boston: Springer. doi:10.1007/978-0-387-37876-3_12

van Eijk, N. (2007). Search engines, the new bottleneck for content access. In *Proceedings of International Telecommunications Society ITS 19th European Regional Conference*, 2-5 September 2007. Istanbul, Turkey. Retrieved March 14, 2009, from http://www.itseurope.org/ITS%20CONF/istanbul2007/index.php?page=abstracts.

van Eijk, N. (2009). A converged regulatory model for search engines? *International. Magazine of the Society for Computers and Law*, *19*(6), 1–3.

Wang, W., Meng, W., & Yu, C. (2000). Concept hierarchy based text database categorization in a metasearch engine environment. In Q. Li, Z. M. Ozsoyoglu, R. Wagner, Y. Kambayashi & Y. Zhang (Eds.), *Proceedings of the First International Conference on Web Information Systems Engineering (WISE'00)* (Vol. 1, pp. 283-290). Hong Kong, China.

Wang, Y., & DeWitt, D. J. (2004). Computing PageRank in a distributed Internet search system. In *Proceedings of the 30th VLDB Conference* (pp. 420-431). August 29-September 3, Toronto, Ontario, Canada. Retrieved January 27, 2009, from http://www.vldb.org/conf/2004/RS11P1.PDF.

WebSideStory. (2004). *Google's search referral market share reaches an all- time high.* Resource document. Retrieved February 2, 2009, from http://www.websidestory.com/pressroom/press-releases.html.

Webster, F. (2006). *Theories of the information society* (3rd ed.). London: Routledge.

Wellman, B. (2001). Changing connectivity: A future history of Y2.03K. *Sociological Research Online, 4*(4). Retrieved January 21, 2009, from http://www.socresonline.org.uk/4/4/wellman.html.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM*, *46*(8), 91–95. doi:10.1145/859670.859675

Wielki, J. (2008). The impact of search engines on contemporary organizations- The social and ethical implications. In T. W. Bynum, M. Calzarossa, I. Lotto & S. Rogerson (Eds.), ETHICOMP 2008: Living, Working and Learning Beyond Technology (pp. 769-803). Mantova: University of Pavia, Italy.

World Summit on the Information Society. (2003). *Declaration of principles: Document WSIS-03/GENEVA/DOC/4-E, 12 December*. Resource document. International Telecommunications Union. Retrieved April 5, 2009, from http://www.itu.int/wsis/docs/geneva/official/dop.html.

Zeller, T. J. (2006). A new campaign tactic: manipulating Google data. Resource document. *The New York Times (Late Edition (East Coast))*, 20. Retrieved February 28, 2009, from http://www.nytimes.com/2006/10/26/us/politics/26googlebomb.html.

Zhang, Y., Vasconcelos, W., & Sleeman, D. (2004). Ontosearch: An ontology search engine. In M. Bramer, F. Coenen & T. Allen (Eds.9), *Proceedings of the 24th SGAI International Conference on Innovation Techniques and Applications of Artificial Intelligence* (pp. 58-69). Cambridge, United Kingdom.

Zien, J., et al. (2001). Web query characteristics and their implications on search engines. In *Proceedings of the 10th WWW International Conference.* May 1-5, Hong Kong, Hong Kong. Retrieved January 25, 2009, from http://www10.org/cdrom/posters/1077.pdf.

Zook, M. A. (2005). *The geography of the Internet industry venture capital, dot-coms, and local knowledge (Information Age Series)*. Oxford: Blackwell Publishing.

ENDNOTE

[1] Deep Web or Dark Matter are also expressions for this concept