Privacy, Data Pollution, Organizational Responsibility, and the Sustainability of Information Ecologies

by

Rob Nehmer, Ph.D.
Associate Professor
Oakland University

Marilyn Prosch, Ph.D, CIPP
Associate Professor
Arizona State University

November, 2009

Privacy, Data Pollution, Organizational Responsibility, and the Sustainability of Information Ecologies

Abstract

The literature on business and sustainability has been sparse to date. Theory building in the domain has been especially scarce. One-pillar models emphasize an ecological dimension to sustainable development. These models talk about sustainability in terms of the reduction of pollution and the sustainability of ecological environments without regard to human usage. That is, they emphasize sustainability from a “natural” point of view. Multi-pillar models, most of which are newer and appear post 2000, are usually the so-called three-pillar models. The usual pillars in these models are ecological, economic, and social. Each of the three pillars, the ecology, the economy and society, are often considered as separate, yet interconnected, systems. To this we add consideration of four distinct different theoretical perspectives that have been employed to study privacy. The four perspectives are 1) design science and technical, 2) individual privacy and consumer behavior, 3) strategic, operational and financial, and 4) societal and public policy. In the area of various types of environmental pollution, modeling is very advanced in the natural sciences and a large research stream exists. Modeling pollution in "information economies" is scarce, perhaps even non-existent. Thus, we assert that contaminants that exceed normal levels in data can be referred to as "toxic data" in information system ecologies. We propose a digital ecology comprised of resources, economic activities, and society. Each component of this ecology is a system in its own right. The system of natural resources consists of the available goods on the planet and their interrelationships where the goods are both living and non-living. The economy is the system of interrelated human activities which affords humans the means of sustaining their basic physical well-being across generations. Society is then the system of interrelated human activities which allow humans to maintain their psychic well-being across generations. The interactions among the three systems produce and re-produce an ecology of human and non-human, living and non-living interactions. The digital ecology models some of the underlying complexity of this natural ecology. Even at this relatively early stage of the development of this digital ecology, its own complexity and risks become an area of concern, especially in matters of privacy. In the paper, we attempt to model privacy responsibility within a corporate model, and then from there, we believe it makes sense to tie this concept of corporate privacy responsibility into the greater societal aspect of social responsibility. The model is based on the Dillard and Layzell’s (2008) model. The model is divided into 3 areas: motivating forces, operational modalities and outcomes. Since the major stakeholders in current economic societies are organizations and individuals, we develop a model of organizational privacy that we then use as a backdrop to develop a model of privacy, data pollution, and sustainability.

Privacy, Data Pollution, Organizational Responsibility, and the Sustainability of Information Ecologies

1. Introduction

The literature on business and sustainability has been sparse to date. Theory building in the domain has been especially scarce. One-pillar models emphasize an ecological dimension to sustainable development. These models talk about sustainability in terms of the reduction of pollution and the sustainability of ecological environments without regard to human usage. That is, they emphasize sustainability from a “natural” point of view. Multi-pillar models, most of which are newer and appear post 2000, are usually the so-called three-pillar models. The usual pillars in these models are ecological, economic, and social. Each of the three pillars, the ecology, the economy and society, are often considered as separate, yet interconnected, systems. To this we add consideration of four distinct different theoretical perspectives that have been employed to study privacy. The four perspectives are 1) design science and technical, 2) individual privacy and consumer behavior, 3) strategic, operational and financial, and 4) societal and public policy. In the area of various types of environmental pollution, modeling is very advanced in the natural sciences and a large research stream exists.

Modeling pollution in "information economies" is scarce, perhaps even non-existent. Thus, we assert that contaminants that exceed normal levels in data can be refer to as "toxic data" in information system ecologies. We propose a digital ecology comprised of resources, economic activities, and society. Each component of this ecology is a system in its own right. The system of natural resources consists of the available goods on the planet and their interrelationships where the goods are both living and non-living. The economy is the system of interrelated human activities which affords humans the means of sustaining their basic physical well-being across generations. Society is then the system of interrelated human activities which allow humans to maintain their psychic well-being across generations. The interactions among the three systems produce and re-produce an ecology of human and non-human, living and non-living interactions. The digital ecology models some of the underlying complexity of this natural ecology. Even at this relatively early stage of the development of this digital ecology, its own complexity and risks become an area of concern, especially in matters of privacy. In the paper, we attempt to model privacy responsibility within a corporate model, and then from there, we believe it makes sense to tie this concept of corporate privacy responsibility into the greater societal aspect of social responsibility. Since the major stakeholders in current economic societies are organizations and individuals, we develop a model of organizational privacy that we then use as a backdrop to develop a model of privacy, data pollution, and sustainability.

The paper develops in this way. First we discuss the social sustainability and privacy literatures. Next, we consider the current state of the art concerning society, public policy, and privacy. Then the paper explores the relationships between privacy and the economy since the economy is one of the fundamental systems in social sustainability. Then we introduce and evaluate the concepts of pollution and data pollution, after which we define organizational privacy responsibility. We then use these descriptions to develop a model of privacy, data pollution, and social sustainability.

2. Social Sustainability Research

The literature on business and sustainability has been sparse to date. Theory building in the domain has been especially scarce. Dillard and Layzell (2009) performed a deep textual analysis of one company's Corporate Responsibility Report. From a theory building perspective, their paper is interesting because it conflates social sustainability with corporate responsibility. According to the authors "(T)he terms *corporate responsibility* and *sustainability* are used, but the term *social sustainability* is not officially part of the formal vernacular…The two phrases dance around each other, but generally coalesce around the term *corporate responsibility*." Their paper then concentrates on exploring the self divulged information reported by the Intel Corporation in the areas of education, the community, and the corporation itself. While this is a useful approach in examining voluntary corporate disclosure, it is less helpful in providing a grounding of social sustainability in business contexts.

As we continue to explore possible theoretical underpinnings for sustainability, we can consider whether and how sustainability is taught. In some cases, teaching actually leads practice and we may consider sustainability to be a good candidate for this since it has generally been a development pushed by less powerful interests. Following this leads us to volume 1 of *Teaching Business Sustainability: from Theory to Practice* (2004). This collection of papers contains additional guidance in the search for theories of sustainability. Foot and Ross's (2004) paper "Social Sustainability" in that volume sees the beginnings of a three-pillar model in the Brundtland Commission's definition of sustainable development, which is that it "meets the needs of the present without compromising the ability of future generations to meet their own needs" (p. 107). The Brundtland Commission was formed by Oxford University to investigate social sustainability in the 1980's. This definition adds an intertemporal characteristic to sustainability. Foot and Ross see social sustainability as being driven by two factors. The first factor is the need for the society to sustain its ecology in order to be able to preserve the ecological matrix in which it has developed and maintains itself. The Cary Institute of Ecosystem Studies defines ecology as "the scientific study of the processes influencing the distribution and abundance of organisms, the interactions among organisms, and the interactions between organisms and the transformation and flux of energy and matter." The second factor is the economic (business) need for going-concern business opportunities within cultural contexts. They promote the idea of a triple bottom line, first developed by Elkington, where the development of long term metrics in the areas of economics and finance, the ecology, and society becomes a driving force behind the movement towards sustainability. In their view, one of the most significant problems with this is the creation of these metrics, especially for social sustainability. From an economic and financial point of view, the metrics should correlate with risk reduction and the creation of business value. This triple bottom line idea is very similar to a balanced scorecard approach where the typical financial measures are supplemented with additional metrics for associated domains, typically operations, customers, and employees through organizational learning. A fairly extensive body of research on the balanced scorecard approach exists in the accounting literature. Using this literature in conjunction with what is available in the sustainability area will be explored in this paper in subsequent sections.

Another paper in the *Teaching Business Sustainability* collection is by Elliott *et al* (2004) entitled "Approaching Sustainability through a Business-Science Synthesis." This paper suggests a paradigm shift in business. This shift is from a view of the world in which business exploits the environment and shifts the externalities to future generations to one where "profitability and environmental responsibility are treated as complements rather than substitutes" (p. 151). In the authors view, this shift will be driven by consensus building activities involving business, citizens, and the political system. Each group will continue to act in its own self interest while also giving consideration to the larger system. Unfortunately, the authors do not provide a prescriptive approach to the operationalization of their shift in paradigms.

A third paper of interest in this volume is "Teaching Sustainability: Whole-Systems Learning" by Brown and Macy (2004). The authors provide a prescriptive method for teaching sustainability principles through what they term "the work that reconnects." The essentials of this work are to help people reconnect to what the authors call the self-correcting, self-organizing powers of living systems. Once this is accomplished, the student is in a position to "seek out, create, and apply sustainable business practices within the workplace and the larger world" (p. 219). This is done through a series of exercises. These exercises are designed to help people in the following areas. First, they are designed to help them to understand the costs of externalizing business and human costs of production. Second, they are designed to share personal experiences of these costs. Third, they provide a reframing of the distress in their lives caused by these externalities. Next, they provide experience in system science concepts and their application to daily life. Fifth is the exploration of personal responsibility to past and future generations of all life. Finally, the exercises help people clarify their intentions. A further method is used which unblocks feedback loops typically ignored in day to day human interactions. The method consists of recognizing mutuality, integrating painful information, expanding perceptual horizons, and finding creative responses.

The final paper of interest in the volume is "Sustainability in a Business Context" by Wood *et al* (2004). The authors recommend that sustainability be integrated into the business' strategic objectives. They present a process diagram with the following components. First, of course, the business must develop its strategic business objectives. Following that, the objectives are aligned with the focus on organizational learning objectives, much like a capability maturity model. Next there is the intellectual capital engine which consists of five pillars discussed below. Finally, the acceptance of real-time business sustainability projects will lead to measurable business results which can be fed back into the strategy process. The five pillars in this model represent the investment in intellectual capital and the existing process designs. The first pillar is business alignment which includes strategic leadership, effective communication and fact-based decision-making, among others. The argument here is that sustainability can be used as a rationale for business continuity and strategic leadership. The second pillar is sustainability knowledge. This includes a type of activity sometimes known as environmental scanning. It is the knowledge of the current state of the art in sustainability and the ability to forecast new developments as they evolve in the field. The third pillar is personal and organizational leadership. This includes purpose-driven leadership, visionary foresight and personal mastery. Not surprisingly, the details of how these items are to be operationalized are not clearly stated in the article. The fourth pillar is systems thinking. Systems thinking is defined here in terms which hearken back to the 1960's. The main ideas are synergies and holistic, relational connections between the parts of the system. Also included here is the recognition that all systems are evolving and an appreciation of the role played by human mental models in helping to create the future. The fifth and final pillar is the enabling technology and processes. The emphasis here is on equity, transparency, and mutual benefit. Equity implies that all parties enjoy respect and equal status. Transparency refers to the requirement that the parties are all engaged in an open process devoid of gaming. Mutual benefit means that the connections between parties are known and understood. The material in this paper also lends itself to integration into a model of sustainability which we develop below.

Another paper on social sustainability, Littig and Griessler (2005), looks at social sustainability from a more theoretical approach. Littig and Griessler begin their discussion with the Brundtland report (WCED, 1987) and the Rio documents (UN, 1992). They discuss one-pillar and multi-pillar models of sustainability development. One-pillar models develop directly from the WCED and UN reports and emphasize an ecological dimension to sustainable development. These models discuss sustainability in terms of the reduction of pollution and the sustainability of ecological environments without regard to human usage. That is, they emphasize sustainability from a "natural" point of view. Multi-pillar models, most of which are newer and appear post 2000, are usually the so-called three-pillar models. The usual pillars in these models are ecological, economic, and social.

Continuing with the discussion of three-pillar sustainability models, Littig and Griessler point out that each of the three pillars, the ecology, the economy and society, are often considered as separate, yet interconnected, systems. Additionally, little consensus has been reached on what constitutes the society pillar. Often times other terms, especially culture and the political system, are made into separate categories distinct from the social pillar. From a theory building perspective, this leaves us with some problems. Indeed, Littig and Griessler point out that there are strong dichotomies between such constructs as social concerns versus social learning as well as science and politics in this area. They point out the need for an integrated sustainability theory which incorporates the ecology, the economy as well as society. Interestingly, their paper then emphasizes what is actually a two-pillar model of society and nature where society now includes the economic, political and social systems.

3. Privacy Literature Review

Much research on privacy has been conducted from many different perspectives. Before we review the literature, we will begin with a definition of privacy and its components. The AICPA has defined privacy as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and destruction of personal information." (GAPP, 2009) GAPP is based on Fair Information Practices and legislation from around the world, and it has 10 Principles which are good guidance for protection of information: Managment, Notice, Choice and Consent, Collection, Use and Retention, Access, Disclosure to Third Parties, Security, Quality, and Monitoring and Enforcement. The dimensions of information privacy put forth by Smith *et al*. (1996), namely, the collection, unauthorized secondary use of information inside and outside of the organization, errors, reduced judgment, and data combination, closely align with GAPP. This alighnment indicates that the academic communities and industry agree somewhat on the basic parameters of privacy. However, drilling down into ownership issues and operationalizing these dimensions given business needs, social desires, technology and legal contexts makes it a very challenging area.

Recently, two studies have developed research frameworks and synthesized prior research (Boritz *et al*. 2008 and Kauffman *et al*. 2009). The approaches are similar at first glance, but do have some dimensional differences. Boritz *et al*. (2008) examine Internet privacy, while Kauffman *et al*. (2009) examine enterprise-wide privacy. Boritz *et al*. (2008) develop a framework and review the literature organized around three main entities: customers, companies and government. Kauffman *et al*. (2009) develop a framework that represents five different kinds of stakeholders – individuals, organizations, privacy-enhancing solution providers, regulators and standard-setters,and independent assurance providers. Both studies place the customer as the center of focus and both have the government/regulators/standard setters as a main entity/stakeholder. Kauffman *et al*. (2009), however, separate privacy-enhancing solution providers from other organizations, while Boritz *et al*. (2008) has those two groups of stakeholders combined into one entity. One key difference between the studies, however, is that Kauffman *et al*. (2009) include a second key dimension in their framework. They consider the "variety of *theoretical perspectives* that are applicable to the analysis of information privacy." They identify four distinct different theoretical perspectives that have been employed to study privacy. The four perspectives are 1) design science and technical, 2) individual privacy and consumer behavior, 3) strategic operational and financial, and 4) societal and public policy. Because we believe the theoretical perspectives add rich context, we will primarily focus on the Kauffman *et al*. (2009) framework, with a focus on the financial and societal and public policy perspective as these most closely align with the economic and societal pillars of the proposed ecological model of information We also consider technologies as being embedded in these perspectives, and the technological issues will be discussed within these sections. Further because both Boritz *et al*. (2008) and Kauffman *et al*. (2009) provide such comprehensive literature reviews, we limit our discussion to only those studies most relevant to this study.

3.1 Society, Public Policy and Privacy

Privacy has been considered one of the four ethical issues of the information age (Mason 1986); the others are accuracy, property and access, which are also very closely related to issues of data pollution. Dillard and Yuthus (2002) assert that the "privacy of personal information is among the most volatile and difficult issues of the information age representing one of the most immediate dilemmas facing AIS." Warren and Brandeis (1890) wrote a seminal article with a legal perspective that contended that "[p]olitical, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society." Warren and Brandeis (1890) wrote their article when they were outraged by the ability of photographers with new mobile cameras to take photographs on the street without the permission of individuals. Technologies continue to advance, more and more rapidly, and such concerns arise with the introduction of each new technology. At the time Warren and Brandeis wrote their article, mobile cameras were extremely large, heavy and obvious compared to today's cameras, which even reside on mobile phones. Today, many types of new technologies impact an individual's privacy.

Westin (1967) extended the perspective of Warren and Brandeis (1890) with a book that expressed a socio-political perspective on personal privacy. After providing a comprehensive analysis of the origins of privacy and its role in society, Westin (1967) called for four privacy-related areas of inquiries:

1. Privacy must be defined rather than simply invoked, and its psychological, sociological, and political dimensions must be described on the basis of leading theoretical and empirical studies.
2. New techniques of surveillance, their present uses, and their future prospects must be described, forsaking Orwellian imagery for hard facts.
3. The ways in which modern societies like the United States have reacted to the new surveillance techniques must be examined in depth to see what has been happening to the social norms for privacy, and whether there are trends among interest groups and in public opinion that may help to guide American policy-makers.

4. A discussion of how American law has dealt with the issue of privacy and surveillance is necessary, as the backdrop for an analysis of specific measures that public and private authorities might take to ensure the continuation of privacy as a cornerstone of a social liberty.

We assert that these four areas of inquiry reflect pressing issues for the 21st century, just as they did over half a century ago.

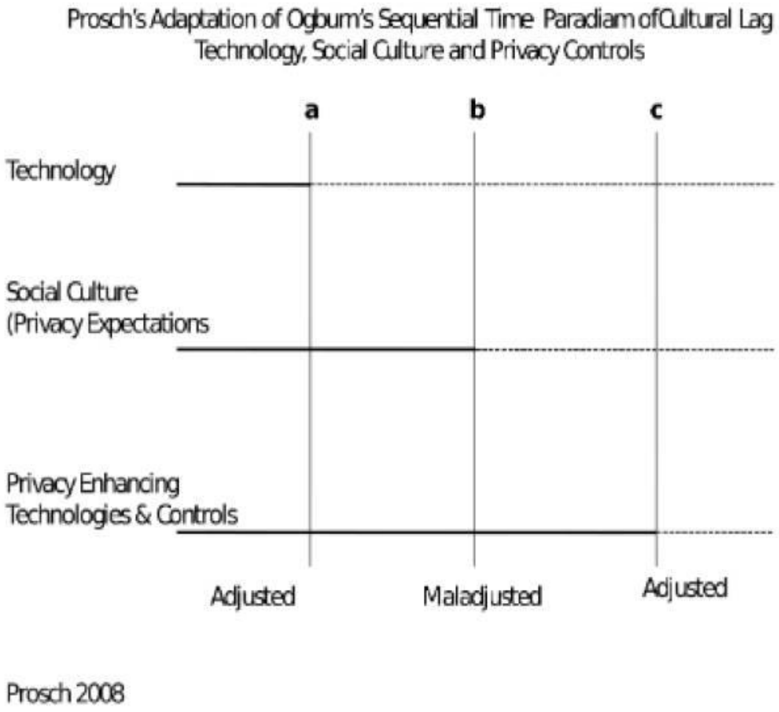


Figure 1

Westin's third point above regarding social norms and the fourth point about American laws being the solution to protecting privacy leads us to consider cultural lag theory, but in so doing, we do not just consider it in a legal context. We consider legal and regulatory actions as one of many possible privacy enhancing solutions. Cultural lag theory is important to the current study because it provides a context to assess whether society is indeed in a period of maladjustment and points out the need for action to be taken for sustainability of the original expectations of culture. The alternative is that adjustment never occurs and culture changes forever. Ogburn (1957) in his proposal of a *cultural lag theory* astutely observed that it takes time for a society's culture to catch up with rapidly changing technology. Prosch (2008) adapted the theory to reflect the interplay of technology, users and culture. The theory has also been tied in to data privacy issues as illustrated in Figure 1. Although the technological advances and resulting maladjustment will affect all of the stakeholders discussed by Kauffman *et al*. (2009), individual expectations with respect to privacy protection will tend to lag behind the development and implementation of technologies that may exploit their private data. Eventually, as individuals learn about the risks, they will begin to demand protection collectively. So businesses, in order to maintain their customer base and be financially sustainable, must react. Theoretically, the privacy-enhancing technology solution providers, and the standards-setting and regulatory stakeholders will react, and begin to deliver solutions and require new privacy-enhancing technologies and privacy-related controls. These actions help to bring the socio-techno-cultural environment back into equilibrium. However, if such action is not taken the previous socio-cultural environment is not sustained and new cultural norms are developed. Boritz *et al*. (2008) and Kauffman *et al*. (2009) both discuss an often hotly debated issue: whether regulation is necessary, or if self-regulation can be effective in the data privacy domain? Kauffman *et al*. (2009) point out that globally, different stances are being taken in different regions. National laws have been enacted in the European Union and Canada, for example, as well as state and provincial legislation. In stark contrast in the US, however, industry-specific laws have been passed in some cases, and a majority of the states, frustrated with laws at the federal level, have passed many of their own laws. Culnan (2000) has reported that only 67% of firms sampled posted privacy disclosures, and that only 14% of the disclosures were considered to be comprehensive. This indicated that a regime of self-regulation might not be effective in producing privacy policies. According to Ogburn's theory we expect to see gradual increases in privacy-enhancing practices over time or as we argue in this paper, culture will be forever changed. The following quote sums up the potential loss of privacy in today's technological culture:

Protecting privacy in the face of ubiquitous data requires many tools: technology, education, market pressure but most of all it requires strong laws that impose serious obligations on industry to act as stewards, not merely processors, of our data, and firm limits on government access to those data. The United Kingdom, under a rigorously independent information commissioner, Richard Thomas, has made important strides in this area. Regrettably, the United States lags farther behind. But we all have a long way to go if we are going to accord individual privacy—the bedrock of human dignity—the respect it deserves. (Cate 2009)

In related research, Solove (2004) provides a detailed analysis of the inter-relationship of individual privacy, society and privacy law. He provides a historical perspective on the conceptualization of privacy problems, their relationship to privacy law and ultimately society. He asserts that "we are still in the early days of the Information Age, and we still have the ability to shape the networks of information flows." This line of thinking is promising from a cultural lag theory perspective. When viewed through a legal lens, he asserts that many of the privacy problems are not really technology driven, rather they are law-related – or the lack thereof – since he argues that privacy to a significant degree is legally constructed. He makes a strong case for this perspective by taking us back to the 19th century and quoting Ralph Waldo Emerson. Mr. Emerson while referring to the mail, declared that it was unlikely that "a bit of paper, containing our most secret thoughts, and protected only by a seal, should safely travel from one end of the world to the other, without anyone whose hands it had passed through having meddled with it" (quoted by Solove 2004, p. 225). In order to protect the post office's mail and to integrate privacy into these practices laws were then created as a response to the relatively new mail system, rather than preserving the status quo. Even with technologies that are considered new to our generation, Solove contends that this can still be accomplished. Cavoukian (2009) agrees with this contention and is an advocate of designing privacy into systems of all types. Security and confidentiality of data has typically been considered as an afterthought in the design and implementation of new technologies and systems. However, over time, a fundamental paradigm shift is occurring, stimulating *Privacy by Design* (Cavoukian 2009), a concept embedding privacy enhancing technologies directly into new systems. Finally, Prosch (2008, 2009) argues that data needs to be protected from cradle to grave, meaning throughout its entire data lifecyle, and most importantly, unnecessary data should never be collected. These important concepts are key to preserving the privacy rights of individuals and as we will argue in the next section, sustaining a culture that values the fundamental right of privacy.

3.2 Privacy and Economics

Cavoukian (2002) touts the benefits to businesses of protecting personal information. However, many organizations do not see the value of deploying resources into privacy enhancing programs. Kauffman *et al*. (2009) point out that although individuals desire to have their information fully protected, organizations are constrained by budget and profit considerations. They acknowledge that full data protection may be socially desirable, but not necessarily feasible for organizations in a competitive environment. Kauffman *et al*. (2009a) find, in their review, that not many studies have examined the economic properties related to privacy issues. They take a risk management approach and assert that the goal of cost-benefit analysis for investments in data privacy solutions is to justify an investment in information security both within an organization and across its inter-organizational boundaries in order to mitigate unnecessary risks. They assert that “risk management theory provides a useful means to justify investments in data privacy protection and information security.”

Value-at-risk theory is an approach for assessing privacy risk. This technique is especially useful when there is the possibility for the occurrence of extremely rare but severe cases of financial loss (Jorion 1997). Both Wang *et al*. (2008) and Kauffman *et al*. (2009b) have used this approach. They utilized value-at-risk to measure the information security risk faced by companies, and applied extreme value analysis or worst-case scenario modeling to estimate the value-at-risk of daily losses. Kauffman *et al*. (2009b) argue from a purely financial perspective that the firm may be inefficiently investing in data privacy protection, both at the low and high end, not investing enough, or investing too much with little additional marginal value for the organization relative to the protection of its customers’ personal information. We contend that analysis needs to be conducted from more than just the firm’s perspective, including that of a societal perspective. Kannan and Telang (2005) found that for network and software vulnerabilities, social welfare is enhanced when the market is regulated (i.e. CERT) and incentives are given to market participants to report vulnerabilities.

4. Pollution and Data Pollution Review

In attempting to derive a meaningful definition of pollution, we begin with exploring various definitions of the term pollution. Princeton University's Wordnet defines it as an "undesirable state of the natural environment being contaminated with harmful substances as a consequence of human activities" and "the act of contaminating or polluting; including (either intentionally or accidentally) unwanted substances or factors". This definition refers to the "natural" environment, and we contend that "information" in the "information age" in which we live is a part of the natural environment. We also see that the unwanted substance or factors may be generated either intentionally or accidentally. The Merriam-Webster dictionary defines pollution as "the introduction of contaminants into an environment that causes instability, disorder, harm or discomfort to the ecosystem i.e. physical systems or living organisms." This definition focuses on contaminants, which can be naturally occurring or man-made. Contaminants are to be expected to some degree, but when they exceed a "normal leve”' they become pollutants.

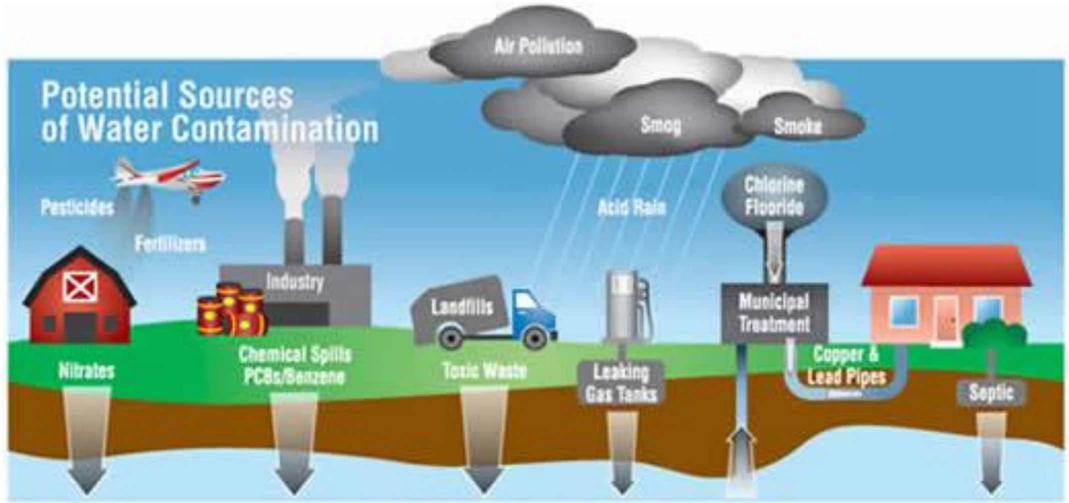
Helfland *et al*. (2003) assert that "pollution occurs because it is virtually impossible to have a productive process that involves no waste; economically pollution occurs because polluting is less expensive than operating cleanly." The industrial revolution which introduced new machines and factories resulted in a huge increase in water, air, soil and even noise pollution. Noise pollution is interesting because is leaves no contaminant residue, rather it disturbs the environment as sounds beyond the "normal level" are contaminating the environment. However, in certain cases, inhabitants of the eco-system can suffer long-term consequences, such as degraded ability to hear, even though the contaminant was only temporary. This is a spot-on example of Ogburn's cultural lag theory, the factories were built, the contaminants were let loose on the ecosystem until they were ultimately brought, at least somewhat under control in certain countries. In the US it resulted in many regulatory acts, including the The Clean Air Act, the Clean Water Act, the Noise Control Act, and the Environmental Pollution Act and the creation of the EPA. Unfortunately, not all countries have brought these forms of pollution under control through regulation. A list of the World's 10 Most Polluted Cities (Linfen, China; Tianying, China; Sukinda, India; Vapi, India; La Oroya, Peru; Dzershinsk, Russia; Norisk, Russia; Chernobl, Ukraine; Sumgayit, Azerbaijan; Kabwe, Zimbabwe) confirms that ecosystems can be greatly damaged when technologies get introduced that produce contaminants and are not controlled.[1]

Helfland *et al*. (2003) attack pollution policies and assert that "environmental goods provide the classic case where government intervention increases efficiency." Achieving efficient levels of pollution involves charging per unit of pollution based on damages caused by that unit. How such emission of pollution fines should optimally be levied when enforcement is costly has been researched for physical pollution (Stranlund *et al*. 2009) and those models have some corollaries with data pollution. In the information economy in which we live, the FTC has indeed issued a few large fines to companies with data pollution in the form of data breaches, and penalties in the HIPAA law also include per infraction fines for data pollution where personal health information is leaked out. In both of these cases, data pollution can be seen as a "leakage" of personal data into the public (non-personal) domain, and in both cases, the metric is the instance of the leakage, that is, the case or individual.

Pollutants can also be categorized as primary or secondary pollutants defined by the EPA as follows. A primary pollutant "is one that is emitted into the atmosphere directly from the source of the pollutant and retains the same chemical form." An example of a primary pollutant is the ash produced by the burning of solid waste. A secondary pollutant is one that is formed by atmospheric reactions of precursor or primary emissions. Secondary pollutants undergo a chemical change once they reach the atmosphere. An example of a secondary pollutant is ozone created from organic vapors given off at a gasoline station. The organic vapors react with sunlight in the atmosphere to produce the ozone, the primary component of smog.

The EPA contends that controlling secondary pollutants is generally more problematic because mitigation requires the identification of the precursor compounds *and their sources* as well as an understanding of the specific chemical reactions that result in the formation of the secondary pollutants. We contend that information ecologies also have primary and secondary pollutants and understanding their relationships and mitigating data pollution as it travels through multiple parties in "cloud" and other types of ubiquitous computing are akin to the increased difficulty of understanding the specific chemical reactions in the natural sciences in the formation of secondary pollutants. For example, when data is transferred among trading partners and combined and further processed we content the white "cloud computing" can quickly become a "brown cloud" of toxic waste. Consider Figure 2 (borrowed from one of NASA's websites).

Figure 2



http://disc.sci.gsfc.nasa.gov/oceancolor/additional/science-focus/locus/images/pollution.jpg

This diagram portrays water contamination, and we can see primary contaminants of 1) nitrates from pesticides, 2) PCBs/Benzene from chemical spills, 3) toxic waste from landfills, 4) gas from leaky tanks, and 5) refuse from septic tanks. We see by-products, however, of air pollutants to be a secondary pollutant that becomes a primary source of water contamination. In the next section, we will use these concepts to set forth a model of data contaminants that, when above normal levels, become toxic and are considered data pollution.

Modelling the various types of environmental pollution is very advanced in the natural sciences and a large research stream exists. Modelling pollution in "information economies" is scarce, perhaps even non-existent. A stream of research does exist on "noise" in data and in data communication channels (Shannon, 1949). Reducing such noise, however, is really just considered to be a data quality issue and is somewhat akin to "normal" contaminants that exist in any ecosystem. Just like we speak of "air quality" the concept of "data quality" has been considered by researchers for some time (Juran 1951; Lee *et al*, 2002; Wang and Strong, 1996; and Wang and Wang, 1996), but again typically at "normal" rather than pollutant or toxic levels.   Thus, we assert that contaminants that exceed normal levels in data can be referred to as "toxic data" in information system ecologies, and this is the topic of this section. The dimensions of data quality put forth by these researchers tend to focus on accuracy, relevance, timeliness, completeness, representational faithfulness, and accessibility.   Quantity of data is not discussed, meaning the propagation of the data and the number of footprints is not a factor, but it is one that we will greatly consider in the context of an information ecology and data contaminants that can become toxic. Relevance is considered an attribute of data quality, but "shelf life" of this relevance and what it means for retention/destruction of the data is not usually considered (Prosch 2008). Again, we need better metrics which move from the existence of an “abnormal” condition to a quantification of the riskiness of that condition.

Now that we have considered the basics of pollution and made a few suggestions towards how data pollution might be modelled, we will review the very few works that have made suggestions of data pollution. Gilb (1980) used the phrase "new industrial data pollution" in the context of a new data processing industry that utilized abstract numeric codes which impeded employee productivity because of their lack of understandability. This work is relevant to data pollution and privacy, as we will discuss in the next section, because in many countries, such as those in the EU, individuals have a right to access their personal information, but if it is given to them in format that is not understandable, then it is useless for that purpose.

Knight (1992) provides evidence that data quality was suffering in large US companies, he called this data pollution. His study provides some interesting historical data of the quality issue, but does not really address the issue of toxic data pollutants. The causes given by him for poor data quality are 1) data entry errors, 2) data entered incorrectly because complete and accurate information was not available at the time of entry, 3) data "mismatched" during merging process, 4) poorly synchronized transaction processing. The first two causes we view as primary contaminants and the second two as secondary contaminants. He asserts the this poor data quality results in 1) violations of SEC reporting, 2) incorrect billing, 3) cost overruns and late deliveries, and 4) product line rework and recalls. Interestingly, the "damage" to individuals are not considered, just "operational" and reporting problems. We will extend the ramifications of poor data quality to privacy and data pollutants in the next section.

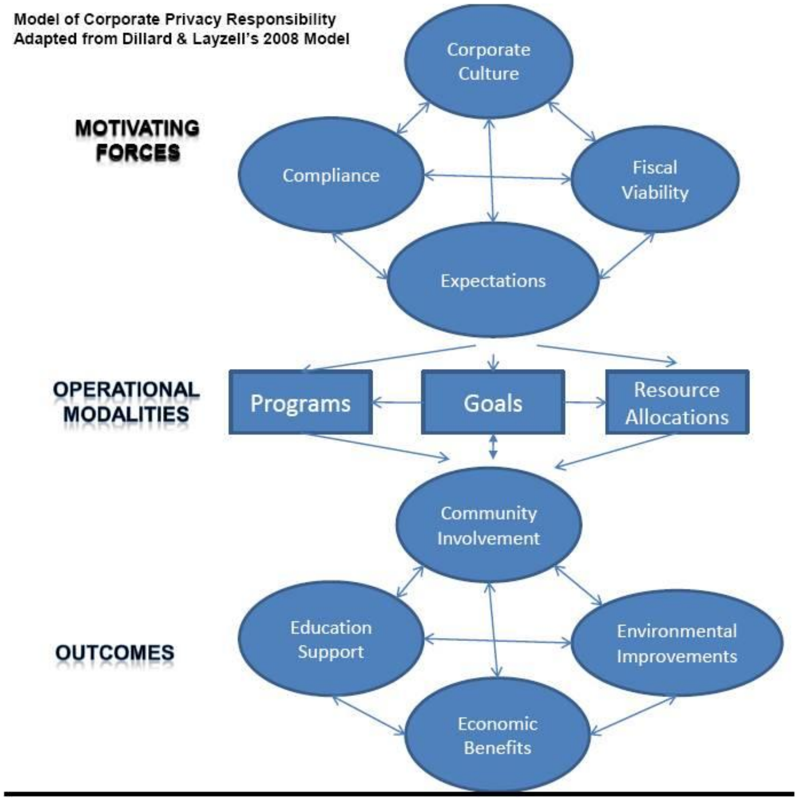
Recently, Brandel (2008) questions whether it is time for a "digital diet" to help reduce "digital pollution" in response to information overload. However, her perspective was from one of data usefulness and information overload rather than "toxic" or harmful data. Schneier (2008) spoke about data pollution, people, and the death of privacy in an interview. The basic thrust of the interview closely aligns with Ogburn's (1957) cultural lag theory as adapted by Prosch (2008). Basically, he asserts that we have as much technology as we need, but security is what is lacking and that security needs to be designed so that it does not require educated users. We propose to take it much further than just security, as we propose the information ecology needs cleaning up and better processes than transcend just security concepts.

5. Organizational Privacy Responsibility

In this section, we develop a model of Organizational Privacy Responsibility[2], and from that model we will next focus in on privacy and social sustainability. As mentioned earlier the differentiation between organizational responsibility and social sustainability has not been very clearly articulated, so we attempt to model privacy responsibility within a corporate model, and then from there, we believe it makes sense to tie this concept of organization privacy responsibility into the greater societal aspect of social responsibility. The resulting model can be seen in Figure 3, and is based on the Dillard and Layzell's (2008) model. The model is divided into 3 areas: motivating forces, operational modalities and outcomes. The 4 motivating forces are 1) Corporate Culture, 2) Compliance, 3) Fiscal Viability, and 4) Expectations. Cavoukian and Hamilton (2002) assert that privacy can only be achieved if top management is on board . Specifically, Cavoukian (2007) asserts that:

1. A culture of privacy enables sustained collective action by providing people with a similarity of approach, outlook, and priorities;
2. The importance of privacy must be a message that comes from the top;
3. Privacy must be woven into the fabric of the day-to-day operations of an organization, with adequate resources.

Figure 3



Interestingly, this definition speaks to the issue of sustainability being enabled by a privacy culture, we will revisit this thought in our next section. What is key to corporate privacy responsibility is that the message come from the top and is designed into every facet of the day to day operations. This concept also ties into Wood *et al*.'s (2004) concept of purpose-driven leadership, with the purpose being to respect and protect personal information.

Organizations are motivated to be in compliance with regulatory and legislative statues because if they do not they face fines, sanctions and even additional required audits. In recent years the US Federal Trade Commission has fairly uniformly required security audits every 2 years for the next 20 years for organizations that are investigated for security breaches and found to be lacking.[3] In Canada, companies have been ordered to have audits and recently Facebook has been ordered to change its practices or shutdown operations in Canada.[4] Similarly, Google is working in Switzerland to enhance its streetview image blurring or it faces being shutdown in that country.[5] Thus, compliance is a compelling motivation force.

Cavoukian and Hamilton (2002) and Cavoukian (2008) have advocated that privacy is an imperative for businesses and that in the long-run it adds value. The third motivating force, fiscal viability can be viewed from a risk approach (Jorion 1977, Wang *et al*. (2008) and Kauffman *et al*. (2009b)) where from a purely financial perspective, a firm may be investing too much or too little in data protection, implying that organizations need to find their "sweet spot" which is where the marginal value for the organization is optimized. Another indicator of fiscal viability is ability to keep market share, and Ponemon (2008) finds that data breaches result in a 3.6% customer churn rate.

Finally, the fourth motivating force is meeting expectations of stakeholders. The primary stakeholder in privacy is the individual Individuals in society wear many hats (employee, consumer, and citizen) and their expectations of privacy may vary across cultures. Prosch (2008) dicusses the relationships between technological advances, societal expectations and resulting privacy enhancing technologies and processes. The expectations of these individuals will ultimately motivate organizations to align their privacy practice with societal expectations, unless society experiences a fundamental paradigm shift in their expectations.

The operating modalities of coporate privacy responsibility are Goals, Programs and Resource Allocations. The program specifics and resource allocations should be driven by the specific privacy goals developed by the organization, which are developed based on the motivating forces or pressures. In privacy, goals may be to merely implement a privacy program or perhaps to move along the privacy maturity model (Prosch 2008). The privacy maturity model is a tangible way that an organization can plot its journey in enhancing its privacy corporate responsibility. Once an organization assesses where it falls along the maturity model, it can then determine where it wants to be in certain intervals of time and set a path to get there. For example, an organization in the early stages of its privacy maturity lifecycle may have as a goal to develop repeatable, measurable privacy practices, such as responding to a request for information in a uniform way. Another organization, further along the maturity model, may have as its goal to "pass" a privacy audit, such as a GAPP audit. Once those goals are defined, the corresponding programs and resource allocations can be determined. What is key is that the motivating forces will drive the goals, and the goals drive the programs and practices and resource allocations.

Finally, the operational modalities will have outcomes, specifically, community involvement, education, economic and environmental improvements. The first outcome will be the degree of community involvement that results. Community involvement involves having programs and policies in place to allow individuals to voice their opinion about their privacy desires. This will only happen if organizations value the opinions of their privacy stakeholders and provide venues (which takes) resources. As indicated in the diagram, the opinions need to provide feedback that is considered in the development/refinement of privacy goals, programs and resource allocation. Metrics here include the existence of programs and policies as well as the percentage of the relevant constituents providing feedback.

Educational support is the second outcome, and organizations should take a proactive role in explaining and training employees on how they are using their data. Sears just recently got ordered by the US FTC to clearly explain to users exactly what data they were collecting and how they were going to use it when they offered to pay them $10 to download software to allow them to track their online browsing data. Most customers thought it was just their general browsing data, when it was actually the secure browsing as well, bank accounts, health information and others.[6] Metrics in this dimension need to map from the organizations' data and policies and procedures to the training and education that the relevant clientele receives.

The third outcome, economic benefits is closely related to the motivating force of fiscal viability, it is just the actual achievement of the fiscal benefits. Metrics are designed for this dimension in a relatively straightforward ways. As one example of such an outcome, customer retention is shown to be higher for banks ranked higher on privacy. The Ponemon Institute finds the average length of a customer relationship for the five banks rated highest for privacy to be

7.68 years, and for the five lowest rated banks, the average relationship length was 4.6 years. Admittedly, the research design did not take into account possibly omitted variables that could be driving the results. However, Cavoukian and Hamilton (2002) assert that aligning an organization's strategies with privacy protecting methods and technologies will pay off in the long run. At this point, this is really still an empirical question.

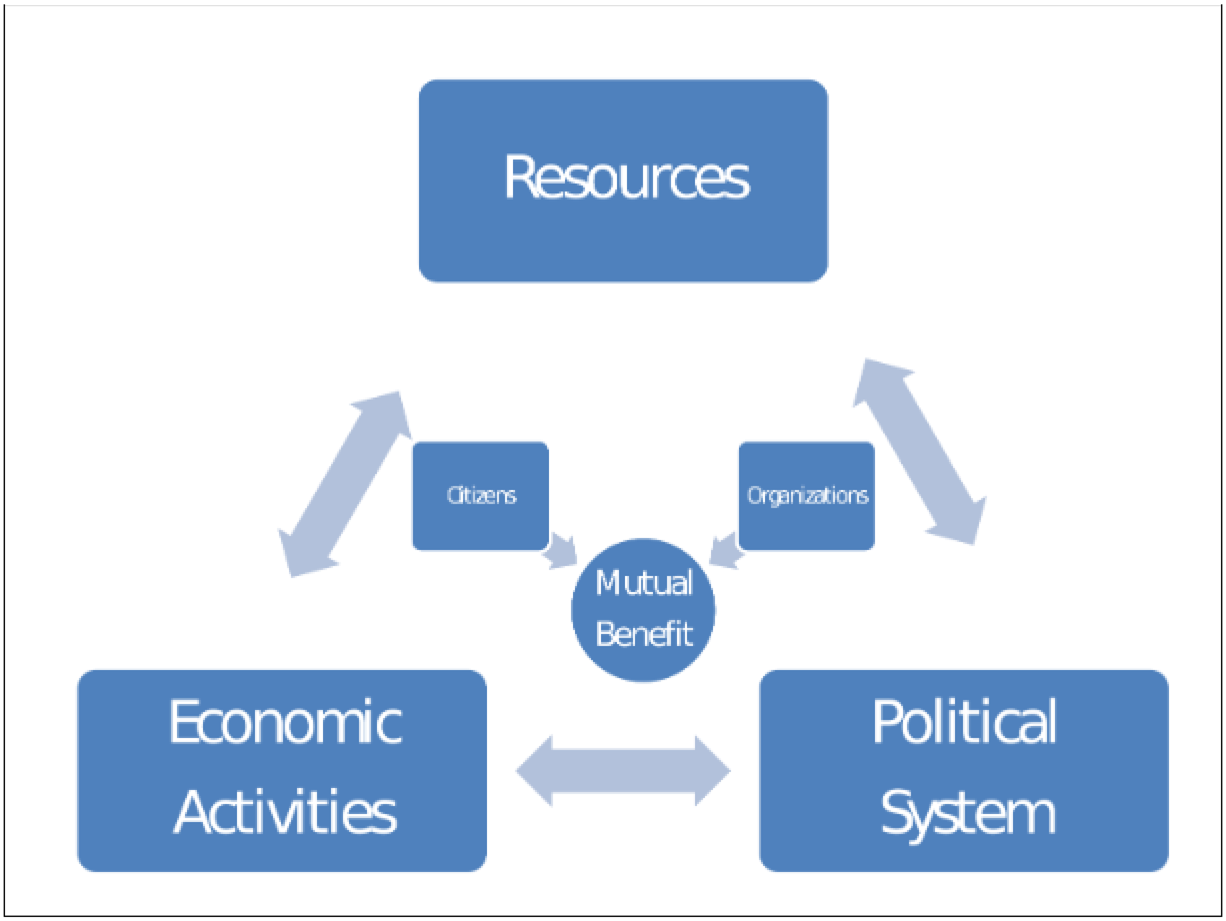
The final outcome, and the primary focus of the next section, is on the environment. As previously discussed, we live in a digital society, but, not everything is digital. We recognize that good data privacy practices have the potential to reduce physical waste in the form of unnecessary paper usage and disk storage devices. We are more focused on the environmental improvements throughout the data lifecycle (Prosch 2008) associated with 1) unnecessary data being collected, 2) data unnecessarily being shared, 3) data being erroneously processed, 4) erroneous data being shared, 5) obsolete data being retained longer than normal, and 6) data being inadequately destroyed. Good corporate privacy responsibility can help to reduce all of these sources of what we term "data pollution" as defined in the next section thereby creating an improvement in the digital economy.

6. Privacy, Data Pollution and Social Sustainability

In this section we drill deeper into the concept of environmental improvement from the organizational privacy responsibility model and draw upon the literature reviewed on social sustainability, privacy and pollution to develop a theory of data pollution in a digital ecology, with a special focus on privacy of personal information. In keeping with Foot and Ross's (2004) notion of a triple bottom line of sustainable ecologies, we propose a *digital ecology* comprised of resources, economic activities, and society. Each component of this ecology is a system in its own right. The system of natural resources consists of the available goods on the planet and their interrelationships where the goods are both living and non-living. The economy is the system of interrelated human activities which affords humans the means of sustaining their basic physical well-being across generations. Society is then the system of interrelated human activities which allow humans to maintain their psychic well-being across generations. The interactions among the three systems produce and re-produce an ecology of human and non-human, living and non-living interactions. For instance, the motivating forces of the organizational privacy responsibility model outlined in the last section are comprised of interaction between the economic and social systems. To the extent that these three systems are modeled as data and information, and their interrelationships measured and, to a certain extent, controlled via information technologies. We then conceive of a digital ecology which models some of the underlying complexity of this ecology. To this characterization, we add the concept from Nehmer (2009) that an information economy is composed of producers and consumers of information. We extend this idea to include parties with both information needs and information producing capacities. The interaction of the parties, corporations, individuals, and regulators within the three systems is what constitutes a digital ecology.

Even at this relatively early stage of the development of this digital ecology, its own complexity and risks become an area of concern, especially in matters of privacy. The primary stakeholders in this proposed ecology are individuals and organizations (Elliot *et al.* 2004) as illustrated in Figure 4. We view the relationship between individuals and organizations as one that is optimized when a positive sum approach (Cavoukian 2009) to privacy is used and mutual benefit (Wood *et al*. 2004) is considered.

Figure 4



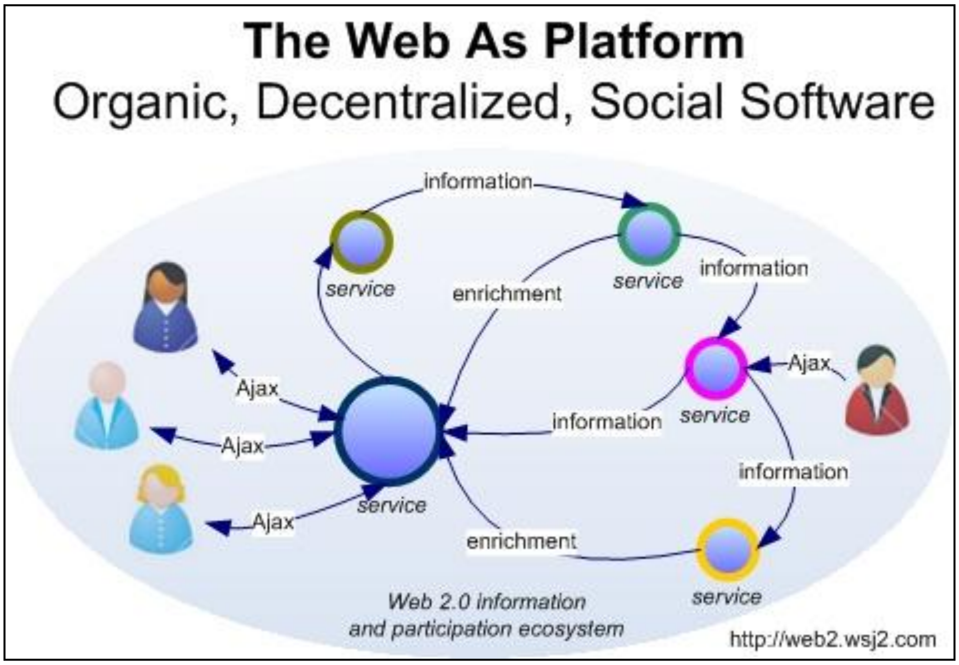
When dramatically new technologies are introduced into society that use up resources and change the nature of economic activities, the challenge is for society to determine whether it desires a permanent change in culture. If not, then the ecology, so to say, needs to adjust, perhaps facilitated by changes made in the political (regulatory) system, economic activities (nature of transactions and processes) and resources (types of technologies employed) to return it to a steady state.

As we begin to consider pollution in this digital ecology, consider the following statement regarding the advent of Web 2.0:

> Essentially, the Web is shifting from an international library of interlinked pages to an information ecosystem, where data circulate like nutrients in a rain forest." (Johnson 2005)

This is an interesting analogy for the flow of data, however, it is really referring to creating efficiencies and reducing information overload in the newer web computing environment. The issue of the exponentially increasing instances of data is illustrated in Figure 5, but data is not considered from a privacy perspective.

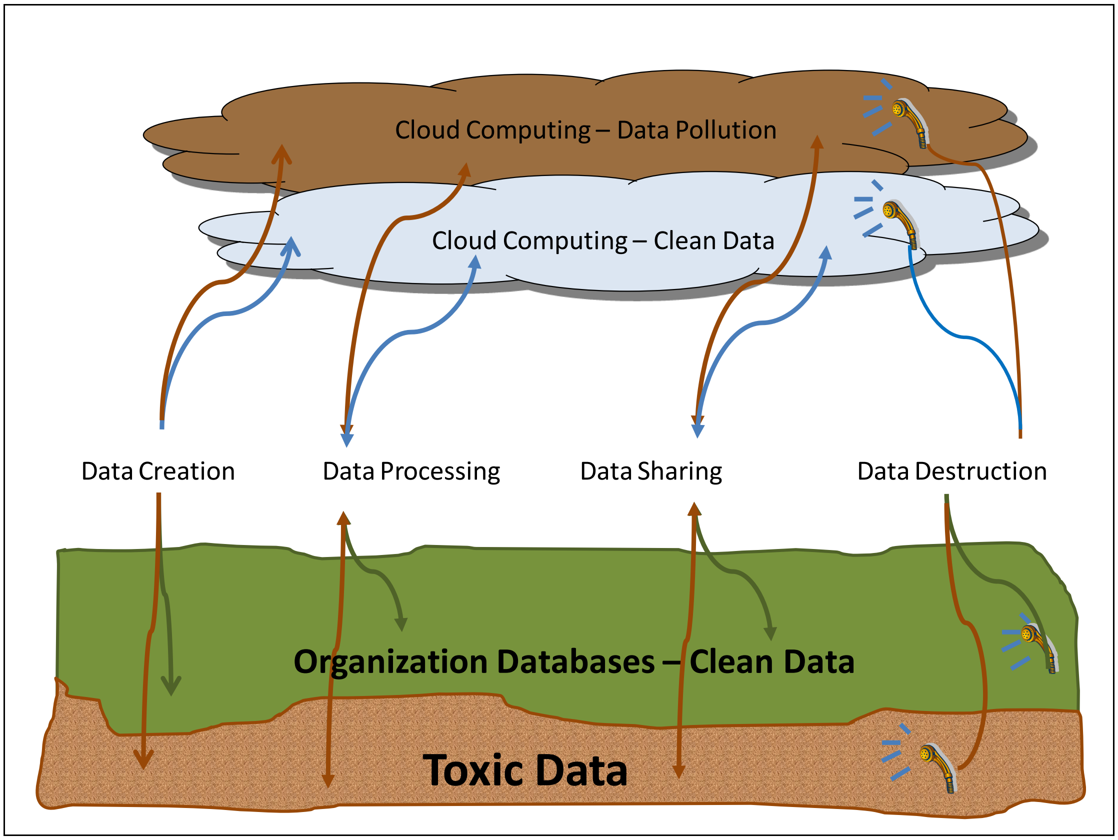
Figure 5



http://web2.socialcomputingjournal.com/describing_the_web_20_information_ecosystem.htm

Continuing with the rain forest analogy, we contend that rain forests can and are contaminated and can be forever changed by various environmental pollutants, as well as deforestation activities. Groups are formed, such as the Save the Rainforest, with the goals of education of the general population and actual protection of the rainforest. Ecosystems need to protect themselves from pollution, and so we consider digital pollution in a digital society. In doing so, we restrict ourselves here to considering only first and second order effects. We realize that there are in fact webs of interrelationships but defer discussion of such complex digital ecologies to further papers. Drawing from the definition of pollution given earlier, we define data pollution as the act of contaminating or polluting; including (either intentionally or accidentally) unwanted data. Where pollution in this case is the introduction of erroneous or unnecessary data into an environment that causes instability, disorder, harm or discomfort to the ecosystem. Potential sources of data pollution can be identified during all phases of the data lifecycle, which is illustrated in Figure 6. In this diagram, we call erroneous and essentially unnecessary data that leaves the organization and travels to third parties of any type “data pollution”, and similar data that stays within the organization “toxic data”. In essence, they are both potentially toxic and pollutants to the environment as a whole. However, because the data within an organization is “contained” within the organization and only hurts society if it is accidentally or maliciously released into the ecosystem, it is potentially toxic, and could be considered by risk management as a contingent liability. The riskiness of this data increases with its overall size and with its potential polluting impact if it enters the public sphere. Data sent to third parties, however, is data pollution, and indeed, it may be toxic. It is immediately considered data pollution because it has left the organization and been released into the ecosystem without feedback to the originating party. Again, metrics are needed to measure both the amount of data released and its negative potential consequences.

Figure 6


Cloud Computing – Data Pollution
Cloud Computing – Clean Data
Data Creation
Data Processing
Data Sharing
Data Destruction
Organization Databases – Clean Data
Toxic Data

Sources of data pollution and toxic data occur throughout the various phases of the data lifecycle. During the data creation phase, special care needs to be taken to only collect data that is necessary. Technologies and cheap data storage makes it tempting for organizations to collect more data than is really needed. Businesses need to identify the business purpose for which data is needed and collect only that data. Collecting other data contributes to data pollution and potentially toxic data, if it subsequently gets misused, lost or stolen. Restricting data collection in this way will significantly reduce the amount of potentially polluting data. Data pollution can also be generated if erroneous data is collected, so data quality is an issue as well. Collection of unnecessary and/or erroneous data can result in both primary and secondary pollution. Secondary pollution would occur if they are used in subsequent processes and cause further toxic data and/or data pollution to occur.

During data processing, new fields of data may be created by inference programming and these fields of data, if not carefully designed and controlled, may result in the proliferation of additional toxins or pollutants. For example, profiling of purchasing habits to categorize individuals with a specific trait and then sharing or selling these inferred traits causes data pollution, which can also be potentially toxic depending on the sensitivity of the categorization, use and security of the data. Metrics need to include indices of the shifts in consumer preferences and the duration of those preferences with corresponding data retention policies.

During data sharing techniques, the problem is controlling the intended use and allowed number and time frame of intended uses. Ensuring that the data is only used for intended purposes without directly observing the usage trail is almost impossible. Finally, data retention should not be “forever” and the data will ultimately need to be destroyed. In some cases, perhaps all instances except 1 instance for an audit trail may need to be destroyed. Determining when data should be destroyed, ensuring all appropriate instances are destroyed, and destroying the data in an appropriate manner must all be considered. Inadequately and inappropriately destroying data causes data pollution and toxic data to proliferate.

Like other forms of physical pollution, regulatory bodies can step in and determine guidelines and control mechanisms. Similarly, globally, data protections laws have abounded, but not all jurisdictions have equivalent data standards, driven in part by culture, and not all laws and regulations are necessarily enforced. Another motivating force to clean up data pollution can be driven by society demanding such protections and organizations seeking methods to enhance data protection at all phases throughout the data lifecycle. Finally, good organizational governance practices lead to appropriate policies and metrics for controlling the organization’s exposure to data pollution. Organization’s can develop balanced scorecard measures of data privacy pollution using the four outcomes of the organization privacy responsibility. For example, the community involvement dimension measured by the percentage of people responding to requests to opt out. The educational support dimension needs to measure the mapping between an organization’s privacy policy declarations and the training outreach it provides on those provisions. The economic benefits dimension can measure customer retention and satisfaction. The environmental improvements dimension has six sub-dimensions, each with a privacy interpretation. First, we can measure the reduction in collected data. Next, we measure the reduction in data sharing without stated and measurable goals. Third, the overall assurance of proper processing controls is needed using a framework such as COBIT. The fourth dimension is measurable by the reduction of reported data errors in shared data. Fifth is measurable initially by better definitions of useful data life. Finally, the sixth sub-dimension is measurable again by better methods for defining old data and purging that data.

7. Conclusion

We have reviewed a diverse literature in sustainability, privacy, and pollution in order to begin to understand and measure a sustainable data ecology. Drawing on the works of Dillard and Layzell (2009), Cavoukian (2002, 2007, 2009), Foot and Ross (2004) and others, we develop a model of such a sustainable ecology and some of the metrics it will need in order to be operationalized. The processes that create, process, share and purge data all have the potential to create data pollution. Organizations need to develop policies, procedures and metrics to reduce both the amounts of data that they put through these processes but also the risk of data leakage in each of the processes.

Limitations of the current research include primarily its exploratory nature. There is little research at present in the areas of organizational responsibility, sustainability, and the digital ecology. The present work is a first look only. Additionally, the analysis presented here considered only primary and secondary effects of privacy pollution concerns in the digital ecology. More realistically, models of digital ecologies need to recognize the complex web of interrelationships among the three systems in order to fully represent the complex dynamics of these ecologies.

References

AICPA. 2009. Generally Accepted Accounting Principles. AICPA: New York.

Boritz, J.E., 2008. W.G. No, R.P. Sundarraj. 2008. “Internet Privacy in E-commerce: Framework, Review and Opportunities for Future Research,” *Proceedings of the 41st Hawaii International Conference on System Sciences*.

Brandel, M. 2008. "Information Overload: Is it time for a Digital Diet," *Computerworld Management*, print version, need vol and issue.

Brown, Molly and Macy, Joanna. 2004. Teaching Sustainability: Whole-Systems Learning. In *Teaching Business Sustainability*. Chris Galea (ed.). pp. 218 - 228.

Cary Institute of Ecosystem Studies, Defining Ecology, http://www.ecostudies.org/definition_ecology.html.

Cate, Fred. 2009. “Internet Privacy: Mind Your own Business,” *The Journal*, April, 27, 2009. Issue 22.

Cavoukian, A.. 2007. ”How to Instill A Privacy Mindset and Enhance Your Communications,” A Presentation to the International Association of Business Communicators, October 2007.

_____. 2009. *Privacy by Design*. Published by the Information Privacy Commissioner’s of Ontario.

Cavoukian, A., and T. Hamilton. 2002, *Privacy Payoff*, McGraw-Hill.

Culnam, M.J. 2000. Protecting privacy online: Is self-regulation working? *Journal of Public Policy and Marketing* 19(1): 20-26.

Dillard, J. and D. Layzell. "Social Sustainability: One Company’s Story," A Working Paper. 2009.

Dillard, J. and K. Yuthus. 2002. "Ethics Research in AIS," in Researching Accounting as an Information Systems Discipline, American Accounting Association: Sarasota, Florida.

Environmental Protection Agency. 2009 website. Air Pollution Control Course. http://www.epa.gov/apti/course422/ap2.html

Elliott, Steven R., Gorman, Raymond F., Krehbiel, Timothy C., Loucks, Orie L., Springer, Allan M. and Erekson, O. Homer. 2004. Approaching Sustainability through a Business-Science Synthesis. In *Teaching Business Sustainability*. Chris Galea (ed.). pp.151 - 155.

Foot, David K. and Ross, Susan. 2004. Social Sustainability. In *Teaching Business Sustainability*. Chris Galea (ed.). pp. 107 - 125.

Gilb, T. 1980. "Humanized Computers: The Need for Them and the Substantial Pay-Off," *Computers and People*. Vol. 29, Iss. 5/6: 7.

Helfland, G. Berck, and T. Maull. 2003. "The Theory of Pollution Policy," in *Handbook of Environmental Economics,* Vol. 1: 249-303. Elsevier B.V.

Johnson, S. 2005. "Software upgrades promise to turn the Internet into a lush rain forest of information teeming with new life," *Discover*. October, 2005.

Jorion, P. 2000. *Value at Risk: The Benchmark for Controlling Market Risk*. McGraw-Hill Professional Book Group, Blacklick, OH.

Juran, J. 1951. *Quality Control Handbook*. McGraw-Hill. New York, NY.

Kauffman, R.J. Y.J. Lee, M. Prosch, B. Shao, and P.J. Steinbart. 2009. "Theory and Research Directions for The Study of Consumer Data Privacy: A Stakeholder Analysis," Working Paper, Arizona State University.

Knight, B. 1992. "The Data Pollution Problem," *Computerworld*, Vol 26, Iss. 39: 81.
Lee, Y.W., D.M. Strong, B.K. Strong, and R.Y. Wang. 2002. "AIMQ: A Methodology for Information Quality Assessment," *Information Management* 40(December); 133-146.

Littig, Beate and Griessler, Erich. Social Sustainability: A Catchword between Political Pragmatism and Social Theory. *International Journal of Sustainable Development* (2005, 8, Nos. 1/2, pp. 65 - 79).

Mason, R. "Four Ethical Issues of the Information Age," *MIS Quarterly* 10(1): 5-12.

Nehmer, R. 2009. "Agent Modeling of Information Assurance," Review of Business Information Systems, 13(3): 17-24.

Ogburn, W. F. 1957. Cultural lag as theory. *Sociology and Social Research*, 41: 167-174.

Ponemon. 2008. 2008 Most Trusted Companies for Retail Banking Study. Ponemon Institute.

Ponemon. 2007. US Cost of a Data Breach. Ponemon Institute.

Prosch, M. 2008. Protecting personal information using Generally Accepted Accounting Principles and continuous control monitoring. *International Journal of Disclosure and Governance* 5 (2): 153-166.

Prosch M. 2009. "Preventing Identity Theft Throughout the Data Life Cycle," *Journal of Accountancy*, 207(1): 58-62.

Schneier, B. 2008. "On People, the Death of Privacy, and Data Pollution," EDUCAUSE Review, 43(2): 12.

Shannon. C.E. 1949. The Mathematical Theory of Communication. Urbana, IL:University of Illinois Press.

Smith, J., S. Milbert, and S. Burke. 1996. "Information Privacy: Measuring individuals' Concerns about Organizational Practices," MIS Quarterly 20(2): 167-197.

Solove, D. J. The Digital Person: Technology and Privacy in the Information Age. New York University Press, New York, NY, 2004.

Stranlund, J.K., C. A. Chávez, and M.G. Villena. 2009. "The optimal pricing of pollution when enforcement is costly," *Journal of Environmental Economics and Management*. Vol. 58, Iss. 2; pg. 183.

Teaching Business Sustainability. Chris Galea (ed.). 2004. Greenleaf Publishing: Sheffield, UK.

United Nations (UN) (1992) Agenda 21, New York.

Wang R.Y., and D.M. Strong. 1996. "Beyond Accuracy: What Data Quality means to Consumers," *Journal of Management Information Systems* 12(Spring): 5-34.

Wang, Y. and R.Y. Wang. 1996. "Anchoring Data Quality Dimensions in Ontological Foundations," *Communications of the ACM*, 39(11): 86-95.

Wang, J., A. Chaudhury and H.R. Rao. 2008. "A Value-at Risk Approach to Information Security Investment. *Information Systems Research* 19(1): 106-123.

Warren, S., and L. Brandeis. 1890. The right to privacy. *Harvard Law Review*, 4(5): 193-220.

Westin, A. 1967. Privacy and Freedom. Atheneum: New York, NY.

Wood, Kathleen, Bobenrieth, Maria, Yoshihara, Faye M. 2004. Sustainability in a Business Context. In *Teaching Business Sustainability*. Chris Galea (ed.). pp. 253 - 267.

World Commission on Environment and Development (WCED) (1987) *Our Common Future*, Oxford University Press, Oxford.

Endnotes

[1] http://www.time.com/time/specials/2007/0,28757,1661031,00.html

[2] We prefer the term organization rather than corporate because it is more inclusive.

[3] See FTC Orders against BJ's, ChoicePoint, CVS, DSW, among others. http://ftc.gov/privacy/privacyinitiatives/promises.enf.html

[4] PIPEDA Case Summary #2009-008: CIPPIC v. Faceboook Inc.

[5] www.the.register.co.uk/2009/09/15/streetview_switzerland/

[6] FTC. File No. 082 3099 Sept. 9, 2009.