The end of forgetting: Strategic agency beyond the panopticon

Jonah Bossewitch
Columbia University, USA

Aram Sinnreich
Rutgers University, USA

Abstract

The rapid explosion of information technologies in recent years has contributed to a substantive change in the social dimensions of information-sharing, and is forcing us to revise substantially our old assumptions regarding the knowledge/power dynamic. In this article, we discuss a range of strategic information-management options available to individuals and institutions in the networked society, and contrast these 'blueprints' to Foucault's well-known panopticon model. We organize these observations and analyses within a new conceptual framework based on the geometry of 'information flux', or the premise that the net flow of information between an individual and a network is as relevant to power dynamics as the nature or volume of that information. Based on this geometrical model, we aim to develop a lexicon for the design, description and critique of socio-technical systems.

In recent years, the digitization and databasing of sociocultural information has led to a glut of data that upends traditional knowledge/power dynamics. Older models of structure and agency based on the presumption of informatic scarcity are giving way to

Corresponding author:
Jonah Bossewitch, CNMTL, Columbia University, 505 Butler Library, 535 West 114th Street, New York 10027, USA
Email: jonah@ccnmtl.columbia.edu

newly emergent forms and practices centered around shaping the flow of information, influencing knowledge production mechanisms, and efficiently assimilating and exploiting oceans of data. In other words, social power is not only premised on what is concealed, it is increasingly constituted in the act of revelation, and in the methods by which we collect and reveal information to and about ourselves and others.

We have seen these new dynamics play out in a variety of highly publicized political and social events in recent years, from Iran's 'Twitter Revolution' of 2009 (Keller, 2010), to Wikileaks' 2010−11 publication of a quarter-million sensitive and classified diplomatic documents (Shane and Lehren, 2010), to the 'hacktivist' denial-of-service attacks (e.g. 'Operation Payback': Mackey, 2010) and document leaks (e.g. incriminating Bank of America emails: Rushe, 2011) undertaken by the group known as Anonymous (Coleman and Ralph, 2011). In response to these kinds of informatic assaults on previously secretive institutions, some have hardened security and attempted to tighten their perimeters (Zureik and Salter, 2005), while others have adopted a strategy of 'radical transparency' (Clemmitt, 2010), presumably in an effort both to capitalize on the distributed intelligence of today's networked information-seekers, and to forestall such attacks.

These rapid shifts in the informatic practices of organizations and institutions in the network society are forcing social actors and theorists to reevaluate their traditional understanding of the knowledge/power dynamic, and to rethink the role that information plays in the sociopolitical sphere (Lyon, 2007). In short, our society requires new models of communication that capture the contours and tradeoffs of informatic transparency and opacity. To put it another way, Foucault's (1995) metaphor of the panopticon, though still relevant (Elmer, 2003), needs to be supplemented by a wider range of architectural blueprints.

This article attempts to provide such a set of blueprints, disentangling the related discourses surrounding transparency, privacy and surveillance by introducing the concept of 'information flux'. The resulting models provide us with the concepts and language to conduct a more productive debate over the struggles to control information flows, and to better understand the personal, social and cultural implications of these outcomes. Although the authors name these blueprints according to the abstract sociographic heuristics we have developed to represent them (e.g. 'Black Hole', 'Promiscuous Broadcaster'), we also relate them to a range of actual and theoretical cultural practices (e.g. the 'quantified self' movement, Face Painting) in order to demonstrate their concrete relevance and applicability.

Thus, the authors aim to articulate a space of behavioral possibilities that encompasses the broad spectrum of communicative choices available in an era we describe as 'The End of Forgetting'.[1] These possibilities are not merely descriptive but strategic in nature, and are calculated to provide both scholars and activists with a lexicon to demonstrate the range of options that now exists for all individuals and institutions throughout the networked society. Awareness is a precondition for action, and in this article the authors aim to demonstrate how our theoretical abstractions are useful for analyzing communicative behaviors, situating these behaviors within a range of possible choices and contexts, and in turn, providing a context for deliberate action. We believe that, in the face of the communication infrastructure's increasing scope and complexity, individuals will require simple and effective models of participation to avoid paralysis and to catalyze strategic agency.

The end of forgetting

Remembering has always been a primary function of media, dating back to the invention of the alphabet and writing (Plato, 1999). Software is especially good at this function, and the digital era can be understood as the cultural absorption of a general technique for representing data *and processes* in a manner that can be stored, retrieved and reproduced. Although the challenges of long-term digital preservation are formidable, purging digital records is an effort which can actually cost more than it saves (Mayer-Schonberger, 2009). Unlike matter or energy, information does not obey any conservation laws; it can be shuffled around and duplicated freely without affecting the original (Barlow, 1996; Siegfried, 2000). Thus, with duplication, transmission and storage costs approaching zero, tracking down and deleting information that has already been released to the world at large can be a Sisyphean effort.

The relationship between recent social trends in surveillance and transparency and the concomitant improvements in the technologies of representation, storage and access is undoubtedly complex. Attempts to establish fixed causal relations between cultural practices and their technological counterparts are often challenging, as these categories ultimately represent different aspects of unified phenomena (Bijker, 2001). For instance, dramatic improvements in record-keeping can be correlated with dramatic shifts in the rate and volume of information flow. Yet the direction, quality and volume of these flows clearly suggest profound implications for power dynamics on both interpersonal and macro-social scales.

Increasingly, machines function as cognitive prostheses, and communication media inch ever closer to approximating the phenomenology of lived experience. Records continue to extend, evoke and replace our experience of memories and, in many ways, digital records are already more faithful than actual memory. Yet, unlike memories, records are effectively permanent, part of an ever-growing archive (Gandy, 2006). But if the end of forgetting is upon us, we must also ask who is doing the remembering.

The political impact of these sociotechnical changes is becoming increasingly apparent, as various constituencies maneuver to increase the flow of information in their direction. Citizens and advocacy groups like the Sunlight Foundation are clamoring for more transparency in government and the private sector, even as it has been discouraged at times by the government itself (e.g. *Judicial Watch* v. *U.S. Secret Service* [Civ. Action No. 06-310; D.D.C.], a recent case in which the White House fought to keep visitor logs secret in the face of Freedom of Information requests). Governments and corporations continue to invest heavily in the apparatuses to surveil, analyze, predict and influence the behavior of their citizens and customers (Mattelart, 2010). Repressive regimes around the world have operationalized these systems in ways that pose grave new threats to activists and human rights (Morozov, 2011). Organizations of all kinds are clamoring for increased intra-network transparency in their communications, often at the expense of individual privacy.

Perhaps no segment of society has more thoroughly internalized these new dynamics than youth culture. Today, most young people (and an increasing number of adults) throughout networked society volunteer an ever-growing volume of personal data, from the mundane to the profound, using services such as Facebook, Foursquare and Twitter.

This behavior resembles transparency, but the asymmetrical control over the so-called 'data exhaust' is cause for concern. Though boyd and Hargittai (2010) have shown that 'the majority of young adult users of Facebook are engaged with managing their privacy settings on the site at least to some extent', the scope and functionality of these privacy settings is limited, unclear and frequently revised. And, with lawmakers and consumer advocates clamoring for federal oversight of Facebook's consumer-tracking practices (ElBoghdady and Tsukayama, 2011), there is little question that the power dynamic over personal data and information continues to place an ever greater degree of control in the hands of marketers and aggregators.

Aside from the obvious concerns this development poses regarding privacy and exploitation, it also raises the specter of a deeper, ontological crisis. Historically, members of our society have taken for granted that we know more about our lives than any third party possibly could, and this knowledge has been vital to our sense of ourselves. The fact that digital databases can now tell volumes more about us than we know about ourselves suggests that the very process of identity-construction is in distress (Yesil, 2005).

Information flux

These competing flows of information exchange are happening within a rapidly changing social context. While individuals, communities and institutions negotiate the directional flows of information, the sheer amount of information being exchanged continues to escalate. The vast number of records that are being collected, correlated and analyzed will have a strong impact on personal and organizational identity, irrespective of the net direction of information flow. However, while the rise in informatic volume seems increasingly inevitable, the net direction of its flow remains to be decided. This open question − who is doing the remembering? − is an essential component of the emerging knowledge/power dynamics.

The physical sciences make frequent use of a measurement known as flux: the rate of flow of 'stuff' passing through a given surface. The flow of particles, fluids, heat and electro-magnetic fields can all be quantitatively described by this analysis, yielding valuable generalizations and predictions (Feynman, 1970). The description of this flow has a geometric representation that is useful for imagining the logical space of possibilities. Many physical laws have been formulated based on the direction, rate and net passage of stuff across the boundaries of the surfaces being studied (Maxwell, 1954; Newton, 1999).

This model, represented as information flux, may also be helpful for conceptualizing the shapes and qualities of emerging information societies. While the sheer quantity of information changing hands is certainly an important factor in understanding the current transformations, equally important are the relative rate at which various individuals send and receive information (Sinnreich, Chib and Gilbert, 2008), the gradient of the information flow, and whether the flux is outgoing or incoming.

Consider our 'personal information clouds' as metaphorical enclosing surfaces (Lamming and Flynn, 1994). The information flux represents all the information that passes through this boundary. If current trends continue, we will soon face a reality in which data collection, storage and analysis are ubiquitous and pervasive. However, these

capacities are not likely to be evenly distributed and there are already major variations in the net flux of information and the capacity to derive meaning from it (Lyon, 1994; Mattelart, 2010; O'Harrow, 2005; Stanley and Steinhardt, 2003).

Simply put, regardless of the quantity or nature of the information being captured, information flows can be divided into three broad geometrical outcomes: (a) positive flux − you are leaking information, and others have access to more than you do, (b) negative flux − you gather and retain more information than you emit, (c) neutral flux − everyone has equal access to everyone else's information, a situation one could describe as a form of perfect transparency.

The terms 'positive' and 'negative' flux are not intended to be normative, or to signify any ethical or strategic value. By mathematical convention, *positive flux* leaves a closed surface, and *negative flux* enters a closed surface. Positive information flux is not necessarily a bad thing, and negative information flux is not necessarily good. In some circumstances, leaking information can be benign or even desirable, provided the person absorbing the information can be trusted. As Nippert-Eng (2010) illustrates through rich and detailed ethnographies, sharing secrets and confidences is inherently social and often used to foster intimacy. Children have negative flux in relation to parents, patients in relation to doctors, sometimes students in relation to teachers. If these authorities have good intentions, these relationships can work well. Parents, teachers and doctors can also be terribly dangerous if they have malicious or unethical intent. As a society, we try organizationally to restrain the power of such information-rich actors, as well as governments and corporations, in order to keep them honest and socially beneficial. Regulations such as the Children's Online Privacy Protection Act (1998), the Family Educational Rights and Privacy Act (1974) and the Health Insurance Portability and Accountability Act (1996) are all policies intended to protect individuals by legislating control over information flux.

A corollary of this detailed and permanent history is an increasing ability to predict, foretell and manipulate future behavior (Gandy, 1993). Additionally, variations in the information flux, and in the expertise and resources to analyze this information, will determine who has access to these predictions. One can also extend the fundamental unit of analysis from an individual to a community or an organization, and describe the information flux within and across the boundaries of these groups.

The information flux model is a reductionist approximation that intentionally disregards some crucial features in the production of identity and meaning, in order to draw attention to other features. The authors acknowledge that information is produced in context, not in a vacuum, and its meaning is derived from that context. Information is produced within a network, and the reduction of this flow to a two-body problem disregards the information that one node might provide about another to third parties. Information is not synonymous with knowledge, and inferences and interpretations do not flow freely across personal boundaries. Information is not homogeneous or arbitrarily interchangeable, and some pieces of information are far more valuable or private than others. Finally, the value of any piece of information is also variable, as different actors may be looking for different patterns or opportunities. Like a turbulent airflow, the real-world dynamics of information flows are complex – far too complex to apprehend in full detail, hence the need for accessible models.

The information flux model is useful for capturing the contours of the dynamics of knowledge exchange, and provides a language for comparing, critiquing and judging competing forms of communicative strategies. All theories obscure certain features of a phenomenon, and make others more salient. The information flux model is intended to complement other frameworks for evaluating the ethics of information flows in a meaningful context (e.g. Nippert-Eng, 2010; Nissenbaum, 2009. Especially alongside these thicker descriptions, this reductionist instrument is a useful heuristic for identifying and articulating taxonomies of behavioral alternatives to be evaluated within strategic contexts. The model helps to identify blind spots, as well as locate and imagine practices across the space of communicative possibilities. It helps us to contrast radical transparency with its alternatives based on differential access to information flows and computing resources. Furthermore, the information flux model is generative, and is a valuable tool for anticipating and designing future communications platforms. Leveraging the information flux model as a heuristic was vital to our construction of the following taxonomy of strategic blueprints.

Beyond the panopticon

The panopticon is central to Foucault's (1995) analysis of the knowledge/power dynamic and is regularly invoked as a starting point in conversations about surveillance societies (Lyon, 2006a). By using Jeremy Bentham's schematic for a self-surveilling prison as a metaphor for the institutional exploitation of imbalanced informatic relationships across a range of social milieus, Foucault both legitimized the technique of architecture-as-argument and made visible a power dynamic that was at once universally intuited and unacknowledged.

Yet the range of informatic architectures has widened in the decades since *Discipline and Punish* was first published, and some new blueprints must be added to the arsenal. In the past few years, many neologisms have emerged that gesture toward the limitations of the panopticon model,[2] though a complete review of this literature is beyond the scope of this article. Rather than simply adding another term to the mix, the information flux model attempts to provide an overarching framework for situating the traditional panopticon alongside its modern variations. Can we update the panopticon by introducing twenty-first-century building materials? Can we extend the panopticon's analytic utility by substituting glass and mirrors for its concrete and steel, and outfitting the building with closed-circuit television cameras? What might this family of blueprints look like?

Using the flux model, the authors aim to sketch the dimensions of a space of strategic action within this environment on several levels, including individuals, communities, organizations and states. Below, we describe some specific strategies and thought experiments that may help us to clarify the challenges and opportunities surrounding privacy and identity in an information-rich society. These examples are not meant comprehensively to catalog the available strategies, but rather to highlight the diverse range of strategies available. These examples also demonstrate the flexibility and utility of the information flux model, and suggest a systematic agenda for future research.

Traditional panopticon

The traditional panopticon describes a prison where the inmates are surveilled by their guards from above. The inmates know they are being watched, though they do not always know when, and their behavior is controlled by the mere threat of being watched. This standard model of surveillance can be construed as a positive flux of information emanating from the individual outward to the institutions of power (Figure 1). It does not adequately capture the nuances and complexities of multi-directional information flows, but it does correspond closely to Orwellian 'Big Brother' scenarios (Lyon, 1994; Orwell, 1961), which can no longer be considered either speculative or delusional. As the American Civil Liberties Union (Stanley and Steinhardt, 2003) and professional journalists (O'Harrow, 2005) have documented, these architectures are rapidly becoming realities, and must be met strategically by the surveilled population.

Sousviellance society

A flip in the polarity of flux described by the traditional panopticon model occurs when the individual participants disrupt the power relation of the traditional panopticon by collaborating to watch the watchers (Figure 2). S*ousveillance* is a term used to describe the recording of an activity from the first-person perspective of a participant (Mann et al., 2003). The prefix 'sous' is French for 'below', in contrast to 'sur'-veillance, from above. By participating in the surveillance processes (both as surveillant and object of surveillance) actively and transparently, individuals can both mediate and understand the personal information they are transacting, and mitigate the inequity of information flow by surveilling the institutions in return.

This is the strategy undertaken by the protagonists in Cory Doctorow's (2010) novel, *Little Brother*, in which a group of teenage computer hackers, building a virtual samizdat network between the Xbox game consoles in thousands of kids' bedrooms, document
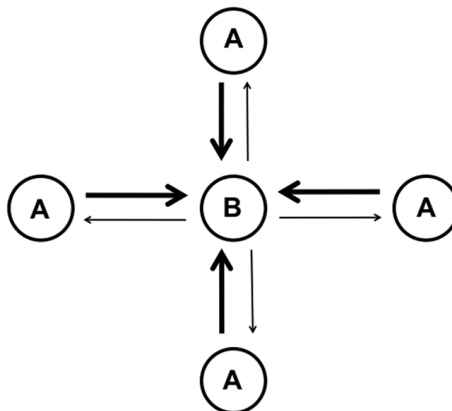

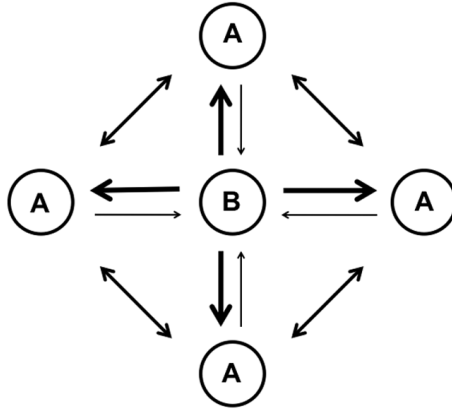
Figure 1. Panopticon.

Figure 2. Sousveillance.

and expose the abuses of power committed by the Department of Homeland Security after they have been unjustly detained and tortured in the wake of a terrorist attack. The power of sousveillance has appeared in the headlines, as well – as when the integrity of a parole officer was questioned by a defendant on the basis of the status updates he published on MySpace (Dwyer, 2009).

Total transparency

This theoretical and unrealizable model describes a world of total transparency in which every person and organization has equal access to one another's information (Figure 3). This corresponds to a neutral information flux, forecast in David Brin's (1999) *The Transparent Society.* This model postulates the end of privacy, but it fails to adequately account for the differential access to analytic processing power available to different individuals and organizations in making sense – and use – of this data.

This strategy is often touted as the solution to institutional corruption, as open government and transparency movements continue to gain momentum and traction.[3] The communications of US presidents must be made available to the public according to the Presidential Records Act of 1974. Similarly, US Federal court proceedings, including depositions, evidence, arguments and rulings must be published in a manner accessible to the public without anyone having to request them, except when the court decides there is a good reason for the records to be sealed.

In the past few decades public policy has shifted from a focus on regulating specific institutional behaviors, toward focusing on broader ethics, such as transparency. For instance, although the Food and Drug Administration (FDA) does not necessarily require that food manufacturers use or ban certain ingredients, it does require them to add ingredient information to their packaging with the expectation that better-informed consumers will influence corporate behavior through their purchasing decisions (Graham, 2002). Some have placed great faith in the power of transparency to improve accountability and,
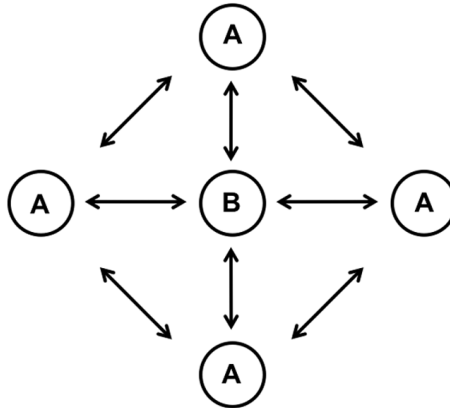
Figure 3. Transparency.

in turn, to exert market pressure on institutional behavior. However, the success of these transparent systems hinges to a large extent on the details of their design.

Off the grid

The 'off the grid' strategy describes efforts to disappear as thoroughly as possible from the information exchange, and to reduce information flux to zero (Figure 4). For the individual, this strategy is enacted by actually disengaging from the telecommunications network, or by encrypting and obscuring the information transacted, and by refusing to use credit cards, mobile phones, ATMs or any of the myriad points of surveillance now encountered in daily life. For instance, Theodore Kaczynski, the infamous 'unabomber', lived in a cabin without electricity or running water in an attempt to disengage from what he called the 'industrial-technological system' ('FC', 1995). Similarly, Gene Hackman's character in the 1998 film *Enemy of the State* (dir. Ridley Scott), an ex-National Security Agency operative named Brill, exemplified the extreme of this strategy, living within a self-constructed copper Faraday cage to shield him from electromagnetic detection.

Black hole

The 'black hole' strategy describes attempts to collect and analyze as much information as possible from the outside, while leaking as little as possible (Figure 5). As profiled in Priest and Arkin's investigative *Top Secret America* (2011), several US intelligence organizations embody this strategy, as domestic eavesdropping programs track and analyze massive volumes of data and metadata. Corporations like Google and Facebook have also built their empires around this strategy (Andrejevic, 2007), underscoring an important point. What constitutes a leakage to users of these sites supports the exploitative black hole strategies of the service providers. One node's 'promiscuous broadcasting' is fodder for another's 'black hole'.
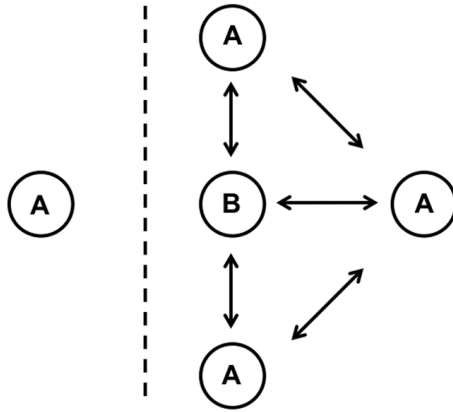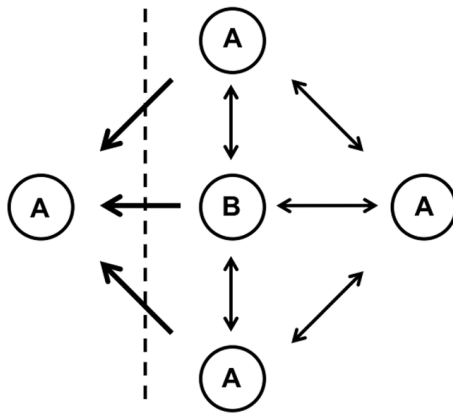
Figure 4. Off the grid.

Figure 5. Black hole.

Promiscuous broadcaster

The 'promiscuous broadcaster' strategy can be practiced non-strategically or strategically depending on the actor's awareness and beliefs. It is similar to total transparency, but does not require symmetrical exchanges of information (Figure 6).

Some individuals ignore the threats of surveillance completely, rationalizing that 'I've got nothing to hide, ergo nothing to worry about', or convincing themselves that the benefits to one's security represented by increased surveillance outweigh the detriments to one's privacy. In today's networked interactive environments, these people are leaking volumes of data (positive information flux). Others may act more deliberately by retaining copies of the information they broadcast. An extreme example of this strategy is Hasan Elahi's 'tracking transience' project. Elahi, a media artist
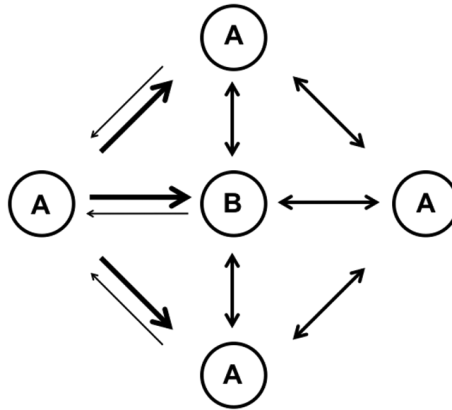
Figure 6. Promiscuous broadcaster.

and Associate Professor at the University of Maryland, was erroneously added to the US government's terrorist watch list in 2002, targeted by the FBI, and subjected to months of intermittent interrogation. His response was to broadcast openly (and also to retain) all the details of his life in a proactive attempt to clear himself of any suspicion of wrongdoing associated with profiling based on his name and/or ethnic background (Thompson, 2007). Elahi makes it clear he views this strategy not as an acquiescence to power, but rather as an act of agency. In his words, 'in an era in which everything is archived and tracked, the best way to maintain privacy may be to give it up' (Elahi, 2011).

Organizations and knowledge communities have also successfully adopted the promiscuous broadcaster strategy, both internally and with outsiders. Academics promiscuously broadcast information in journals, directed at each other, but accessible to anyone. Open source communities often practice radical forms of promiscuous broadcasting, publishing the minutiae of their communications and decision-making processes. In both cases these communications are more complex and varied than a think-tank's or a corporation's messaging. This communications strategy increases the accountability and knowledge-sharing within the community, but may confuse outsiders who are ill-equipped to make sense of these raw exchanges.

Voracious collector

The 'voracious collector' strategy involves maintaining a consistent negative information flux, but it differs from the 'black hole' strategy in not requiring the participant to go partially 'off the grid' (Figure 7). A good way to imagine how an individual might follow this strategy is to consider how the right software might support this practice. The BioPort (Biography Portal) is a piece of 'intension-ware' that we have described in technical detail elsewhere (Bossewitch, 2005). The basic idea for this software begins with a combination blog, diary and appointment book – essentially, a tool for constructing your
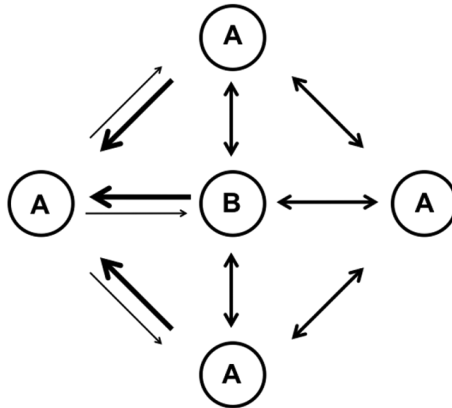
Figure 7. Voracious collector.

autobiography in real time. We can even imagine informational transaction capabilities: just as we receive receipts at the completion of financial transactions, the BioPort could keep track of all exchanges with 'informational receipts'.

To make this fictional scenario more vivid, consider a thin slice of your BioPort − your nutritional history. While Corporations like Walmart and McDonald's might want to use such data to target you with lower-nutrition, higher-margin foods, you would be able to use the same data to make sure your nutritional needs were being met adequately within your budget. Ultimately, you could broker your data to food sellers to negotiate the best balance between nutrition, taste and cost.

The technology would have ramifications for identity-building as well. With the right suite of visualization and analysis tools, the BioPort could become the ultimate psycho-analytic device − one which allows individuals to know themselves better by helping them identify and discern recurring behavioral and informatic patterns in their own lives. It could also transform social spaces, by allowing communities to come together and securely share slices of one another's BioPorts.

Although the BioPort only exists as a thought experiment today, there are projects that represent concrete moves in this direction. For instance, the emerging 'quantified self' movement brings together hobbyists who exchange techniques for collecting and analyzing their own personal data using tools such as the open source Locker Project (Wolf, 2010).[4] Similarly, the Harvard Berkman Center has initiated a Vendor Relationship Management project that implements a flux reversal strategy to help consumers manage their relationships with corporations.[5]

Disinformation campaigns

Another strategy for managing the net flux of information is to propagate *dis*information, thereby reducing the flow of *accurate* information outward and producing a more
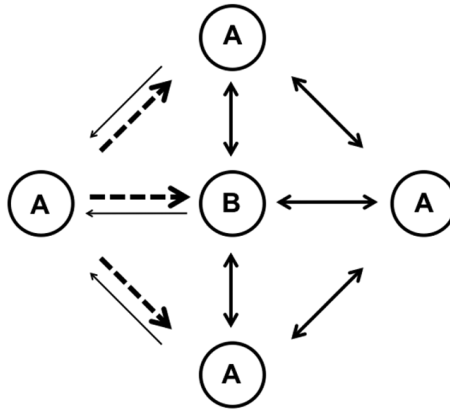
Figure 8. Disinformation.

negative flux overall (Figure 8). This strategy is familiar at the institutional level, in a variety of contexts from political propaganda to advertising campaigns to corporate 'astroturfing' (Beder, 1998; Bernays, 1928).

It also has begun to appear as a strategy for individuals to mitigate the threats of surveillance on social networks (Brunton and Nissenbaum, 2011; Marx, 2003). Face Painting is an underground collaborative game designed to resist the privacy threats that Facebook and other social networks pose. From the *Urban Dictionary*:

> *Face Painting (also referred to as 'MySpin') is internet slang for the practice of sprinkling a social networking profile with embellishments, fantasy, and satire, often with humorous or political intentions. Face painters play with the truthiness of identity by conducting a campaign of misinformation to protect their true identity.*[6]

This obfuscation strategy, though it may appear on the surface to be no more than a mischievous lark, has significant ramifications for information flux. By reintroducing chaos and noise back into the system, Face Painters protect their identities with a campaign of disinformation, and spoof the corporate profiling technologies with odd juxtapositions and preferences. These campaigns also aim to raise awareness around omniscient surveillance, and in particular to critique Facebook's problematic privacy policies. Face Painters have assembled teams for scavenger hunts, recruiting the children of corporate executives to join oppositional causes (e.g. the child of an oil company executive to join an environmental campaign, or the child of a record company executive to join a campaign for progressive intellectual property reform).

Face Painting will not significantly divert the torrential flow of information, but it does cleverly illustrate how individuals can reassert control over their digital footprint, and redirect the net information flux if they are aware of its significance.

Spaces of action

This preliminary catalog of communicative strategies gestures toward the span of choices available to actors in an information-rich environment. The information flux model helps us to discover and situate these strategies in relation to each other. An understanding of this range of possibilities is essential for creating a basis for effective agency and resistance.

Individuals, communities and organizations have very similar options within this space. They can choose actively to receive or ignore the information that flows past them. If they collect the information, they can archive, index and analyze it. They can choose to send or withhold information about themselves. The information they broadcast can be truthful or spoofed.

This spectrum of strategies defines a space of action with varying information flux characteristics. Different strategies offer several routes to achieving a desired value of information flux. For example, negative flux can be increased by voraciously collecting more information or by broadcasting more disinformation. A technology like the BioPort is one way to support individuals maintaining a negative information flux, and continue living in a society where the flow of information is centered around the individual. This social reality is distinctly different than a perfectly transparent society. Prevailing currents are steering the flow of information away from the individual into the waiting hands of those who would benefit from the control over their records and memories. However, one can imagine technologies and strategies that would redirect the flow of information back around the individual and achieve more balance and control over our digital footprints.

Conclusion

Freud (1980) postulated a depth model of psychology in which suppression, repression and the ability to forget are vital aspects of our psychological makeup. These defense mechanisms, which allow individuals to maintain their sense of self, rely upon their ability selectively to recall and subconsciously to filter the personal narratives that are consistent with the reality they want to believe. An individual's ability to cope with trauma and stress depends upon the function of forgetting. The tight relationship between memory and identity has been a mainstay of philosophy and psychology for centuries (Freud, 1980; Locke, 1996; Parfit, 1986). This terrain is most often explored in fiction by examining the ways in which loss of memory alters, compromises or threatens personal and social identity. For example, *The Vintage Book of Amnesia: An Anthology of Writing on the Subject of Memory Loss* (Lethem, 2000) is a collection of short stories that explore these themes across a variety of genres. Numerous films such as *Vertigo* (dir. Hitchcock, 1958), *La Jetée* (dir. Marker, 1962), *Total Recall* (dir. Verhoeven, 1990), *Twelve Monkeys* (dir. Gilliam, 1995), *Enemy of the State* (dir. Scott, 1998), *Memento* (dir. Nolan, 2000) and *Eternal Sunshine of the Spotless Mind* (dir. Gondry, 2004) all grapple with the complex relationship between memory and identity through the device of amnesia. Yet depictions of permanent memory are far less common, with some notable exceptions, including Jorge Luis Borges' *Funes the Memorious* (2007), Phillip K. Dick's *Minority Report* (dir.

Spielberg, 2002) and *A Scanner Darkly* (dir. Linklater, 2006), Arthur C. Clarke's *The Light of Other Days* (Clarke and Baxter, 2000), and Victor Vince's *Rainbow's End* (2007). The personal and social consequences of permanent memory deserve broader and more in-depth examination through art, fiction, social theory and advocacy alike.

Perhaps more troubling than the prospect of memories that cannot be filtered and do not dissipate, is the impact of pervasive surveillance on the social function of deception. Arguably, modern-day society is founded on lies, ranging from niceties between friends and neighbors, to corporate advertising and marketing, to political spin, to the lies people tell themselves to bolster their confidence and support their identities (Frankfurt, 2005; Goffman et al., 1997). Pervasive surveillance threatens to rip apart the fabric of constructive deception that currently weaves together individuals, social groups and nations. The psychological and small-scale social effects of this dynamic can be seen in recent documentaries such as *We Live in Public* (dir. Timoner, 2009) and *Catfish* (dir. Schulman and Joost, 2010), and is detailed in the ethnographies gathered in Nippert-Eng's (2010) *Islands of Privacy*.

The net flux of information flowing into and out of individuals, communities and institutions will have a significant impact upon the emerging models for network society. Depending upon whether the net information flux is negative, positive or neutral, one can see dramatic shifts in the balance of knowledge and power that exists between citizens and governments, between consumers and corporations, and even between individuals.

A positive flux of information from institutions of power to individuals may improve social equality and individual agency by providing accountable checks and balances through distributed oversight. However, the design of these information systems is complicated by the details of representation, storage and access, which can undermine and thwart these balancing forces. Furthermore, reasserting the right to privacy, and even anonymity, may be a central component in sealing the personal information leaks that are distorting the balance in information flux, thereby providing a platform for democratic governance and social equality within an information society.

The exponential growth in the volume of data produced by individuals and institutions shows no signs of abating. The net direction of these informatic flows is hotly contested and continually renegotiated. Just as Gary Marx (2003) cataloged a range of behavioral techniques to neutralize and subvert the collection of personal information, this article catalogs a range of information collection and dissemination strategies that various actors can adopt to purposefully manage their information flows. This catalog is intended to be generative, and can be used to group and apply strategies that might not otherwise be obvious. Using the model the authors have set forth, we can systematically describe and compare informatic strategies and more easily identify tools to support them. For example, we can now describe categorically how the TrackMeNot browser plugin (Howe and Nissenbaum, 2009) enacts and reflects a disinformation strategy (Brunton and Nissenbaum, 2011), and thereby evaluate the strategic benefits of search query logging and spoofing relative to other practices of disclosure and obscurity.

The reductionist information flux model can also play a role in evaluating and gauging the impact of a new technology, and help actors to identify and configure tools that match their intentions. One of the central challenges in formulating a privacy strategy is

paralysis in the face of overwhelming complexity (Barocas and Nissenbaum, 2009). As legislators, corporations and activists work toward clarifying privacy policies, every party will benefit from a clear and standardized lexicon for describing what information is being collected and analyzed, and by whom. Information flux is a critical element of these policies, and our model can play a vital role in formulating such a lexicon.

As networked memory and processing become increasingly central to social architecture, and information flux becomes increasingly vital to power dynamics, the authors have no doubt that a new cultural lexicon will emerge organically to describe the range of strategic options available to actors and institutions seeking to exploit the flow of information to their benefit. In time, these concepts may become second nature to everyone − yet another fact of life in networked society. In the meantime, the authors are confident that the framework we have laid out in this article will provide a useful context for future discussions and analyses by providing a lexicon that enables comparisons across disparate theories and examples, and a heuristic for critique and design.

Funding

Acknowledgments

Notes

1. Although we first introduced this term at the Media In Transition 6 Conference at MIT in 2009, *The New York Times Magazine* used it (apparently coincidentally) as the title of a 2010 article by Jeffrey Rosen on similar themes. The article is available at www.nytimes. com/2010/07/25/magazine/25privacy-t2.html.
2. See Lyon (2006b). For example: (1) synopticon (Mathiesen, 1997); (2) ban-opticon (Bigo, 2005); (3) sousveilliance (Mann et al., 2003); (4) dataveillance (Clarke, 1988); (5) nonopticon (Vaidhyanathan, 2008); (6) netopticon (www.no-org.net/opticon/index.php?m=1); (7) participatory panopticon (Cascio, 2006).
3. For example, the Open Government Charity, http://opengovernment.org/; the Electronic Frontiers Transparency Initiative, www.eff.org/issues/transparency; and the Sunlight Foundation, www.sunlightfoundation.com.
4. http://lockerproject.org/.
5. http://projectvrm.net/.
6. www.urbandictionary.com/define.php?term=face+painting.

References

Andrejevic M (2007) *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: University Press of Kansas.

Barlow JP (1996) Selling wine without bottles on the global net: the economy of mind on the global net. In: Ludlow P (ed.) *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*. Cambridge, MA: MIT Press, pp. 9−10.

Barocas S and Nissenbaum H (2009) On notice: the trouble with notice and consent. In: *Proceedings of the Engaging Data Forum at the First International Forum on the Application and Management of Personal Electronic Information*. Cambridge, MA. Available at: http://senseable.mit.edu/engagingdata/program.html.

Beder S (1998) Public relations' role in manufacturing artificial grass roots coalitions. *Public Relations Quarterly* 43(2): 21–23.

Bernays E (1928) Manipulating public opinion: the why and the how. *American Journal of Sociology* 33(6): 958–971.

Bigo D (2005) The birth of ban-opticon : detention of foreigners in (il)liberal regimes. Paper presented at the annual meeting of the International Studies Association, Hilton Hawaiian Village, Honolulu, Hawaii, 5 March. Available at: www.allacademic.com/meta/p70735_index.html.

Bijker W (2001) Social construction of technology. In: Smelser NJ and Baltes PB (eds) *International Encyclopedia of the Social and Behavioral Sciences*. Oxford: Elsevier Science Ltd, pp. 15522–15527.

Bossewitch J (2005) Becoming your own Big Brother: a paradoxical approach for retaining control of personal freedom. Available at: http://pocketknowledge.tc.columbia.edu/home.php/viewfile/18366.

boyd d and Hargittai E (2010) Facebook privacy settings: who cares? *First Monday* 15(8). Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589.

Brin D (1999) *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* New York: Basic Books.

Brunton F and Nissenbaum H (2011) Vernacular resistance to data collection and analysis: a political theory of obfuscation. *First Monday* 16(5). Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3493/2955.

Cascio J (2006), Earth witness. World changing 3 February 2006. Available at: www.worldchanging.com/archives/004069.html.

Clarke AC and Baxter S (2000) *The Light of Other Days*, 1st edn. New York: Tor Books.

Clarke R (1988) Information technology and dataveillance. *Communications of the Association for Computer Machinery* 31(5): 498−512.

Clemmitt M (2010) Social networking: are online social networks eroding privacy? *CQ Researcher* 20(32). Available at: http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2010091700.

Coleman G and Ralph M (2011) Is it a crime? The transgressive politics of hacking in Anonymous. *Social Text*. Available at: www.socialtextjournal.org/blog/2011/09/is-it-a-crime-the-transgressive-politics-of-hacking-in-anonymous.php.

Doctorow C (2008) *Little Brother*. New York: Tor Teen.

Dwyer J (2009) The officer who posted too much on MySpace. *The New York Times*, 11 March.

Elahi HM (2011) You want to track me? Here you go, FBI. *The New York Times*, 29 October.

ElBoghdady D and Tsukayama H (2011) Facebook tracking prompts calls for FTC investigation. *The Washington Post*, 29 September.

Elmer G (2003) A diagram of panoptic surveillance. *New Media & Society* 5(2): 231–247.

'F.C.' (1995) *The Unabomber Manifesto: Industrial Society and its Future*. Jolly Roger Press. Available at: www.jollyrogerpress.com/.

Feynman RP (1970) *The Feynman Lectures on Physics*. New York: Addison Wesley Longman.

Foucault M (1995) *Discipline and Punish: The Birth of the Prison*. New York: Knopf Doubleday Publishing Group.

Frankfurt HG (2005) *On Bullshit*. Princeton, NJ: Princeton University Press.

Freud S (1980) *The Interpretation of Dreams*. New York: Avon Books.

Gandy O (1993) *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.

Gandy O (2006) Data mining, surveillance and discrimination in the post 9/11 environment. In: Haggerty K and Ericson R (eds) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press, pp. 363−384.

Goffman E, Lemert CC and Branaman A (1997) *The Goffman Reader*. New York: Wiley-Blackwell.

Graham M (2002) *Democracy by Disclosure: The Rise of Technopopulism*. Washington, DC: Brookings Institution Press.

Howe D and Nissenbaum H (2009) TrackMeNot: resisting surveillance in Web search. In: Kerr I, Lucock C and Steeves V (eds) *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press, pp. 417–436.

Keller J (2010) Evaluating Iran's Twitter revolution. *Atlantic*, 18 May. Available at: www.theatlantic.com/technology/archive/2010/06/evaluating-irans-twitter-revolution/58337/.

Lamming M and Flynn M (1994) Forget-me-not: intimate computing in support of human memory. In: *Proceedings of the '94 Symposium On Next Generation Human Interface*, Meguro Gajoen, Japan. Available at: www.lamming.com/mik/Papers/fmn.pdf.

Lethem J (2000) *The Vintage Book of Amnesia: An Anthology of Writing on the Subject of Memory Loss*. New York: Vintage.

Locke J (1996) *An Essay Concerning Human Understanding* (abridged). Indianapolis, IN: Hackett.

Lyon D (1994) *Electronic Eye: The Rise of Surveillance Society*, 1st edn. Minneapolis, MN: University of Minnesota Press.

Lyon D (2006a) The search for surveillance theories. In: Lyon D (ed.) *Theorizing Surveillance: The Panopticon and Beyond*. Portland, OR: Willan Publishing, pp. 3−20.

Lyon D (ed.) (2006b) *Theorizing Surveillance: The Panopticon and Beyond*. Portland, OR: Willan Publishing.

Lyon D (2007) *Surveillance Studies: An Overview*, 1st edn. London: Polity Press.

Mackey R (2010) 'Operation Payback' attacks target MasterCard and PayPal sites to avenge WikiLeaks. *The New York Times*, 8 December.

Mann S, Nolan J and Wellman B (2003) Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance and Society* 1(3): 331–55.

Marx G (2003) A tack in the shoe: neutralizing and resisting the new surveillance. *Journal of Social Issues* 59(2): 369–390.

Mattelart A (2010) *The Globalization of Surveillance*. Cambridge: Polity Press.

Maxwell JC (1954) *Treatise on Electricity and Magnetism*, vol. 1, 3rd edn. New York: Dover Publications.

Mathieson T (1997) The viewer society: Michel Foucault's 'Panopticon' revisited *Theoretical Criminology* 1(2): 215−234.

Mayer-Schonberger V (2009) *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

Morozov E (2011) *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.

Newton I (1999) *The Principia: Mathematical Principles of Natural Philosophy*, 1st edn. Berkeley, CA: University of California Press.

Nippert-Eng CE (2010) *Islands of Privacy*. Chicago, IL: University of Chicago Press.

Nissenbaum H (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

O'Harrow R (2005) *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society*. New York: Free Press.

Orwell G (1961) *1984*. New York: New American Library.

Parfit D (1986) *Reasons and Persons*. New York: Oxford University Press.

Plato (1999) *Euthyphro. Apology. Crito. Phaedo. Phaedrus*. Cambridge, MA: Loeb Classical Library.

Priest D and Arkin W (2011) *Top Secret America: The Rise of the New American Security State*, 1st edn. New York: Little, Brown.

Rushe D (2011) Anonymous hackers release Bank of America emails. *The Guardian*, 14 March.

Shane S and Lehren AW (2010) Leaked cables offer raw look at U.S. diplomacy. *The New York Times*, 28 November.

Siegfried T (2000) *The Bit and the Pendulum: How the New Physics of Information is Revolutionizing Science*, 1st edn. New York: Wiley.

Sinnreich A, Chib A, and Gilbert J (2008) Modeling information equality: social and media latency effects on information diffusion. *International Journal of Communication* 2(1): 1−20.

Stanley J and Steinhardt B (2003) Bigger monster, weaker chains, the growth of an American surveillance society, ACLU Technology and Liberty Program. Available at: www.aclu.org/technology-and-liberty/bigger-monster-weaker-chains-growth-american-surveillance-society.

Thompson C (2007) The visible man: an FBI target puts his whole life online. *Wired Magazine*, 22 May.

Vaidhyanathan S (2008) Naked in the 'nonopticon: surveillance and marketing combine to strip away our privacy. *The Chronicle Review* 54(23): B7.

Vinge V (2007) *Rainbow's End*. New York: Macmillan.

Wolf G (2010) The data-driven life. *The New York Times*, 28 April.

Yesil B (2005) *Blind spots: the social and cultural dimensions of video surveillance*. doctoral thesis, New York University.

Zureik E and Salter M (2005) *Global Surveillance and Policing*. Portland, OR: Willan Publishing.

Jonah Bossewitch is a doctoral candidate in communications at Columbia University and a Technical Architect at the Columbia Center for New Media Teaching and Learning. He writes about surveillance and madness, and is investigating the politics of memory at the intersection of corruption in psychiatry and the pharmaceutical industry. He blogs at http://alchemicalmusings.org.

Aram Sinnreich is an Assistant Professor at the Rutgers University School of Communication and Information. His work centers on the power dynamics surrounding emerging cultures and technologies, and on the policies that regulate these fields. His website is http://aram.sinnreich.com.