The Doppelganger Effect:
Spaces, Traces and Databases and the Multiples of Cyberspace

by

Sandra J. Robinson, BA, MBA

A thesis submitted to the
Faculty of Graduate Studies and Research
in partial fulfillment of the
requirements for the degree of

Master of Arts

Department of Law
Carleton University
Ottawa, Canada

May 14, 2008

Your file Votre référence
ISBN: 978-0-494-40609-0
Our file Notre référence
ISBN: 978-0-494-40609-0

Abstract

The doppelganger effect is a constellation of effects including the ability of databases to reproduce identities out of a collection of facts and minutiae about the natural person. It is a constant and iterative force. The database provides a mechanism for "subject constitution" abstracting the individual from the natural person and creating multiple identities over which the individual has no control. My intent in this thesis is to demonstrate that the very code and structure of databases and of data filtering, aggregation, analysis and profiling operate as a system of production generating the multiples of cyberspace.

Acknowledgments

The genesis of this thesis reaches back many years to work I did in the private sector in the area of intellectual property, software development, and product management within digital technologies broadly. While it began there it has progressed in ways I could not have imagined if not for a rather fortuitous rendezvous with my thesis adviser Prof Sheryl N. Hamilton, CRC in Law, Communications, and Governance at Carleton University, Ottawa. Sheryl, your intellectual gifts alongside your creative and critical engagement with my object of study opened up an experience unparalleled in my professional and academic life to date. I can think of no better way to thank you and repay this debt of gratitude than to continue to pursue an academic life with your standard of academic integrity, originality and generosity in mind.

My committee members, Prof Valerie Steeves and Prof Ira Wagman, provided critical feedback and hearty discussion that has strengthened my work and I thank you for making my defense a positive and stimulating experience. I would also like to thank Prof. Peter Swan, Chair of the Department of Law and Prof. J. Barry Wright for their support.

I toiled in my attic lair day after day and enjoyed every minute of writing this thesis. My happiness in life and success in this project flows from the love and support of RJ without whom I would wither.

Table of Contents

Chapter One

Introduction: The flows and effects of the network society

> As an imagined figure, a soul, a shadow, a ghost or a mirror reflection...the psychological power of the *double* lies in its ambiguity, in the fact that it can stand for contrast or opposition, but likeness as well.[1]

Flows of data are all around us drifting in cyberspace as patterns, connections, and transmissions; we are living in a network society. Data are captured routinely in our daily lives through practices of consumption, production, and surveillance and persist in flows. Flows are referenced in both the literature on surveillance as well as Manuel Castells' theory of the network society to describe *where* data ends up after collection and how it is theorized to *move* throughout the global network (Castells 1996, 470; see also Haggerty and Ericson 2000). It is collected by all kinds of devices including desktop and laptop computers, cell phones, Blackberries, point-of-sale equipment, iPods, garage entry kiosks, TV set top boxes, and car electronics.

The doppelganger effect, like chaos theory's butterfly effect,[2] explains how seemingly innocuous yet organized, orderly events and transactions in cyberspace can result in unanticipated consequences for the natural person. The consequence distills and clarifies into an ordered singularity that, however mistaken it may be, *appears* legitimate: the misidentification of an airline passenger places them on the no-fly list or a financially-established university professor is refused a big-box store credit card. These

---

1 Milica Živković (2000, 122) emphasis mine.

2 The butterfly effect posits that the most subtle change in a nonlinear system will effect monumental change over time due to a sensitivity to initial conditions within the system (Lorenz 1963; Ditto 1995; Bradley 2007). Its popular explanation is that the flapping of a butterfly's wings in one geographic place could alter the initial conditions of a weather system and result in a tornado far away. The metaphor also denotes the shape of the 'lorenz attractor' when plotted graphically (Urry 2006). See also <http://www.pha.jhu.edu/%7Eldb/seminar/butterfly.html> for a thorough scientific explanation.

individuals have a digital doppelganger; their virtual identity or profile constructed from data in the flows is in opposition to their self in the material world. The doppelganger effect need not only be oppositional or a negative consequence although such renderings create a more radical demonstration of the form and effect of personal data in the flows. The doppelganger effect is in perpetual and constant generation as individual identities are written and re-written from personal data collected in databases.

The notion of a double or doppelganger has, in the course of the last five centuries, appeared in western folklore, literature, film and cultural imagination portrayed as a negative or 'evil' entity that presages death of the natural person (Ranald and Ranald 1961, 9).[3] Commonly, fictional portrayals illustrate the doppelganger through "Hostile actions ... ascribed to [a] foreign self ... performed by proxy" (Miller 1985, 25); doppelgangers have a decidedly negative connotation in these fictional landscapes. Discourse around the double is prevalent within Freudian psychoanalysis in studies of the "self within the self" (Vardoulakis 2006).

Otto Rank was intrigued by the double in both Gothic Romantic literature of the nineteenth century and representations in early twentieth century cinema and applied psychoanalytic principles in his studies. He explored many themes in his work on the double such as the "techniques of representation" of the self; the "figure of the independently generated reflection" and the loss of control over one's own image (Rank 1971, 6, 7). Rank's psychoanalytic approach to the notion of the double remains

---

3 Ranald and Ranald (1961, 9-10) note that early works by Ludvig Lavater (1572) and John Aubrey (1696) relate tales of Teutonic and Celtic doubles as staples in folkloric superstition. Sir Walter Scott and Percy Bysshe Shelley both wrote of doubles and Shelley is said to have seen his just before he drowned in 1822 (Ranald and Ranald 1961, 12). Živković (2000, 122) notes the word doppelganger is first believed to have appeared in a work by Jean Paul Richter in 1796 and means 'double-goer' in German.

influential. Contemporary scholars draw on Rank's exposition placing the doppelganger as an object of postmodern literary analysis (Alexander 1997; Labriola 2002). These examinations draw on postmodernism's challenge to the rational, centred self, highlighting the tension between division and unity (Bartlett 2005; Živković 2000). The doppelganger in digital form, I will argue, also appears in the network society implicated in the postmodern disassembly of the self and its themes of multiplicity within cyberspace.

How does the doppelganger effect transpire? The doppelganger effect is stirred into being from the "detritus of contemporary life" (Haggerty and Ericson 2000, 611) persistently and effortlessly captured through day to day transactions. Monitoring, collecting and transmitting personal facts is more and more commonplace among digital devices. Pervasive computing is a proliferating aspect of modern digital technologies in which most electronic devices now carry within them some sort of embedded circuitry and code capable of collecting, sending and receiving data (Wright and Steventon 2006).[4] The aspect of persistence in and of embedded systems is central to this research project. Pervasive computing will collect data from all kinds of places as its sophistication and miniaturization continues to place it in and around our physical environment; however, my thesis will examine the collection of personality-based data from within the home.[5]

How does personality-based data get into the flows from the home? Take the example of a student who logs onto the Internet at home to do her homework. Apple

---

4 Code is commonly defined as a set of rules or programmed instructions that enable and control how all applications, or software, run on a computer, network, printer, cell phone or other digital device (Dodge and Kitchin 2005a). Code can also refer to identification codes such as a social insurance number.

5 Pervasive computing and the Internet itself is based on a distributed computing model whereby flexibility in software is critical to enable systems of relations (connectivity) between objects on the network (printers, servers, PCs) (Power 1990). These systems will be discussed in detail later in the thesis.

iTunes has launched automatically at startup and registered her database of music files on her computer with Apple Inc. matching it to their own song license database. iTunes maintains a persistent link between the student's computer and the iTunes store – it is active the entire time her computer is on (Fisher 2007).[6] The student logs into Facebook.com where dozens of her pictures have been uploaded and countless bits of personal information are posted.

A dozen applications use the Internet connection to send and receive data about software and content running on her laptop; each checks and authenticates software versions and digital content licenses; they log her IP address (her discrete Internet Protocol identifier issued through her Internet Service Provider (ISP)); the time of day; and geographic city location. Every discrete piece of data is logged or recorded by the content provider and stored in a database.[7] Her ISP tracks and archives every email message and instant message.[8]

Persistent connectivity and monitoring in the home provides a networked conduit between private places and market places. Data about individual consumption, utility, place, space and time from within the confines of the home generate personality-based data of a kind and quality not exposed through external market transaction data.[9] I distinguish personality-based data emanating from the home from external market data

---

6 Apple hides personal data in all iTunes files with or without DRM (Ars Technica 2007).

7 There are ample sources for tracing what data is collected by corporations as they manage digital content licensed to an individual user. See CIPPIC (2007) and Microsoft Corporation's documentation on DRM and software product licenses, such as Vista, at www.microsoft.com (various links).

8 Data storage varies according to jurisdiction and data protection directives. See the April 2008 Article 29 Data Protection Working Party opinion on Google data retention practices and Nate Anderson's (2008) comment on Google's retention strategy reduction from 24 months to 18.

9 Ian Kerr and Jane Bailey (2004) examine surveillance capabilities in digital rights management systems (DRM) and argue that personal privacy is threatened by the monitoring features of this technology used for managing access to licensed digital content, e.g. digital music files.

that might include records on health and education, banking data, shopping, insurance and travel history. Information about individuals in the home tracked on personal digital devices reveals intimate knowledge regarding the individual in private life: it reveals what we do in private; when we do it; and how often (J.E. Cohen 2003, 585; see also Kerr and Bailey 2004). The digital doppelganger will look all the more legitimate infused with personality-based data intimating habits, behaviours and preferences of the individual in private life.

The doppelganger effect is a constellation of effects including the ability of databases to reproduce identities out of a collection of facts and minutiae about the natural person. This is a constant and iterative force best described in Mark Poster's "database as discourse" thesis (1996). Poster suggests that the database provides a mechanism for "subject constitution" abstracting the individual from the natural person and creating multiple identities over which the individual has no control (1996, 185). My intent in this thesis is to demonstrate that the very code and structure of databases and of data filtering, aggregation, analysis and profiling operate as a system of production generating the multiples of cyberspace. These multiples are a wellspring for the doppelganger effect.

How, then, does the doppelganger effect manifest in the life of the individual? As the home becomes permeated by pervasive monitoring systems what effect does this have on individual privacy and the space and place of home? As personal information moves from collection to analysis how do databases profile and assemble digital personae and what model of control over the outcome is projected? Where can the doppelganger

effect's traces be encountered in the network society? I will also examine legal solutions centred around protecting personal facts about individuals. By way of conclusion, I ask how legal approaches to informational privacy might contend with the productive power of databases which disrupts the singular, liberal self and renders the subject as an object in/of the flows? The question ultimately is whether the doppelganger effect can be prevented by legal instruments and material controls. These questions guide this thesis.

Information flows: pervasive and distributed

Information flows are central to the story of the digital doppelganger because they contain the mix of data from which it is conjured. Castells defines the network society as one "whose structure is made of networks powered by microelectronics-based information and communications technologies" in which flows or "streams of information between nodes" carry data about people and things circulating in/around/through the network society (1996, 3). He also refers to a "space of flows" that link "electronically separate" geographic spaces (2004, 85).

The notion of global information flows is widely held although different fields of research place an emphasis on different elements of the flows. Surveillance theorist David Lyon defines them with more specificity reflecting the broad implantation of monitoring technologies in society which results in flows of "personal data gleaned from many sources [which] are collected, sold, and resold within the vast repositories of database marketing. These polycentric surveillance flows are ... part of the ... network society" (2003b, 174). Martin Dodge and Rob Kitchin view flows as "coded processes" that facilitate the transfer, access, updating and monitoring of information in relational

databases (2005b, 164). What each of these definitions reveals, however, is a deep dependence on network technologies to facilitate the "coded processes" or flows. Contemporary networks are predicated on the distributed computing model and more and more on pervasive systems operating in the background of the network society.

Pervasive computing made its way into the English lexicon in an article by Mark Weiser ([1991] 1999, 3) outlining computer technology consisting of inexpensive, low power devices networked together that would be part of people's environment and "vanish into the background." Pervasive systems 'sense' environment using a mix of component technology that includes ambient and contextual awareness integrated on one platform connected via a network to other systems effecting ubiquity (Riva *et al.* 2005, 53).

Places and spaces that have pervasive information and communications technology (PICT) embedded in them are composed of "self-contained autonomous processes" connected over a network able to adapt to changing resources and dynamic information flows or the "way information changes through its use" (Power 1990, 2). This is an essential aspect of the distributed computing model itself in which heterogeneous systems, including software, hardware, and communications, must function seamlessly without any centralized control (Power 1992): the backbone of Castells' network society.

Computer science research into pervasive systems readily employs terms such as 'intelligent' and 'aware.' Steve Wright and Alan Steventon (2006) label PICT locations and environments as intelligent spaces, or "iSpaces." Pervasive systems research and development has become modelled on autonomous 'self-processes,' 'smart' systems, and

'human-like' intelligent decision-making adopting a penchant for biological metaphors and anthropomorphic terms (Steventon and Wright 2006).[10]

One of the models for the basis of pervasive and ubiquitous computing is the human autonomic nervous system which is capable of coordinating multiple functions including heart rate and breathing (Shackleton *et al.* 2006, 323). What characterizes human autonomic responses is the amount of information gathered by the brain and, in a healthy individual, a complex feedback cycle to regulate the human body (Rogers 2006). To reproduce even a fraction of that in an artificial intelligence of the kind required in pervasive home systems would require data collection and processing from an array of environmental and spatial sensors. This fact alone has tremendous implications for privacy, personal autonomy, and the security of such private information within a pervasive system (Rogers 2006, 410).

The 'smart home' is replete with terms prefaced by 'self' to describe capabilities modeled on complex biological systems. It is not just in the obvious use of 'intelligence' and 'sentience' to relate the idea that powerful embedded systems in the home can "sense, and make sense of" the environment but that such systems augment the reality of individual experience in the home space (Wright and Steventon 2006, 2).

Home spaces

More and more the home is the site for embedded technologies and research has steered development toward 'smart homes' that have context aware systems (Davidoff *et al.* 2006; see also Intille 2002). The 'smart home' is a pervasive environment, even an

10 The research strays further into biology by modeling algorithms on fruit fly hormones that signal threat responses to counter pervasive network threats; and bacterial plasmid RNA responses to state changes to model 'load balancing' or service requests on a network (Shackelton *et al.* 2006, 325-327).

idealized iSpace (Bull, Limb and Payne 2006): it 'senses' temperature and adjusts; it becomes aware of light levels and adapts; it analyzes household routines and accommodates.

The notion of a 'smart home,' then, is a highly specialized form of home space. Space in these homes has moved from differentiated space to multi-use space in which information and communications technologies (ICTs) and household systems make rooms fully networked spaces. Lynn Spigel has effectively linked the high tech 'smart home' with its sentient code-filled spaces and embedded digital systems to a new mode of subjectivity: 'posthuman domesticity' (2005). Spigel suggests that this new mode invites a new kind of communication: "performative communication" in which individuals demonstrate their communicative acts in cyberspace. The 'smart home' must therefore be connected to the information flows to enable such performative acts.

David Morley opines that "technologies are no longer merely supplementary to, but constitutive of, what the home itself now is" (2003, 450). This assertion is supported by Fiona Allon who suggests that modes of living have morphed from 'private space' to 'media space' (2004, 257). It seems to me that these scholars identify how the home is now, or may soon be, a fully networked space in western affluent countries operationalized as a "node for the circulation of media and information" (Allon 2004, 255). The circulation of media and information is fully two-way and interactive: media and information is routed into the home and personal data about consumption and use is transmitted out to the market sphere.[11] This transformation, then, also places the home in the service of subtle and diffuse modes of governing "at a distance" which relies on

11 Aptly illustrated by Mark Andrejevic's work on peer surveillance and reality TV (2002; 2005).

monitoring and data collection to function successfully.

There is a rich critique of the home as spatially distinct challenging the traditional notion of a fixed boundary around the home. Allon views the smart home as "decentralized, individualized and privatized" leading to domestic space without boundaries which trade network connectivity for increased surveillance (2004, 271). The theme of boundaries, or borders, which establish territories of private and public is challenged by Gary T. Marx as well (2001, 160). He suggests that what appears as a fixed boundary is in fact fluid and diffuse in postmodernity.[12] Morley explores the transformation of the home as a bounded, physical space of belonging to one under pressure from new technologies that change communications patterns and mobility in society (2001, 2003). For Morley, adapting a notion from Zygmunt Bauman, the realms of the far and the near are increasingly mixed up by communications technologies that bridge physical geography and time (2003, 436).

As the home is more and more conceived of and built as a networked space, the spatial sense of privacy as a condition of privacy in the home will be eroded by persistent digital monitoring. Lieven de Cauter views the house as a "plugged-in terminal, a capsule" on the network and he posits that "the degree of capsularization is directly proportional to the growth of Network" (2004, 96-97). He suggests Castells' (2004b) notion of the "space of flows" may be overtaking the "space of place." The "space of place" maintains the notion of a spatially-based location and private place, however,

12 Borders and boundaries to map out the private versus public are also invoked in issues of body surveillance or biometrics. Biometrics "attempt to fix bodies as authenticators of identity in space and time" (Ball 2006, 311) troubling the boundary between bodily integrity and surveillance systems. In this thesis, biometrics does not feature as an object of study, however, the doppelganger effect can be produced by data sources collected by biometric systems mixed with other data.

privacy-invasive technologies in the home will continue to expand in the future with little resistance to their surveillance capabilities. This, I argue, emphasizes a "space of flows" which by necessity must connect to the network in much the way de Cauter's capsule is theorized to do. However, I disagree with de Cauter's notion of capsular as it denotes the potential to remain private through a virtual container around the home. I will argue in Chapter Two that an individualized network connection may be structured to *feel* self-contained but is in fact fully exposed by/through data collection in the home disrupting privacy.

Privacy

Privacy, however, is a complex notion and competing concepts of privacy are not easily explained. The history of privacy relevant to Anglo-American jurisprudence begins with an oft-cited legal commentary written by Samuel D. Warren and Louis D. Brandeis in which they argued for a right of privacy; a "right to be let alone" as a basic principle of human dignity and "inviolate personality" (1890). Warren and Brandeis were particularly concerned with new technologies, such as photography and mechanical newspaper printing, that facilitated intrusion into private life by publishing personal facts and "overstepping in every direction the obvious bounds of propriety and of decency" (1890, 3). This commentary equates privacy with the dignity manifest in "the integrity of one's individual identity and persona" (Kahn 2003, 375). Warren and Brandeis's reflection in 1890 foreshadowed later twentieth century tensions between other 'new' disruptive digital technologies and postmodernism's interrogation of individualistic identity and persona.

Twentieth century legal scholars have sought to find ways to protect privacy and

stabilize it in/under law. There are differences in the approach to privacy between Canada and the United States (McNairn and Scott 2001; Howell 1998). Privacy is not explicitly set out in the *Canadian Charter of Rights and Freedoms* (*Charter*) and the Supreme Court of Canada (SCC) has "employed a general definition of privacy ... [in] connection with other essential democratic values such as individual autonomy, liberty, and bodily integrity" (McNairn and Scott 2001, 2). Privacy has been read into section 8, the search and seizure provision of the *Charter*, wherein "A person who has an expectation of privacy, for the purposes of section 8 of the *Charter* [has] a 'right to privacy'" when subject to an "unreasonable search and seizure" (McNairn and Scott 2001, 18).

Canada has favoured a general right to privacy as per above and a more specific protection of personal information in the private sector under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Very briefly, Canadian courts remain confused over whether to recognize a common law tort of invasion of privacy and in spite of lower court decisions in Ontario finding in this direction neither appellate courts nor the SCC have weighed in on the matter (McNairn and Scott 2001, 45).[13] PIPEDA, overseen by the Office of the Privacy Commissioner of Canada, does allow redress of informational privacy complaints which can be appealed to the Federal Court. The Privacy Commissioner oversees compliance of both PIPEDA and the *Privacy Act* which governs public sector organizations.

In 1960, William Prosser set forth an invasion of privacy tort in four parts and

13 Quebec's *Civil Code* does recognize a breach of privacy and permits recovery for an invasion of privacy (McNairn and Scott 2001, 48).

established a modern mainstay in privacy law used in in the U. S.[14] More recently, U.S. scholars have focused on informational privacy and explored tort-based remedies for unwarranted disclosure of personal facts such as breach of confidence (Litman 2000). Remedy-based approaches to informational privacy have a critical flaw: they are invoked *after* the infraction, after the unwarranted collection, disclosure or circulation of personal facts. In an age of information flows and data sharing, legal remedies for privacy invasions cannot restore a loss of privacy after the disclosure of personal data. The leaked data cannot be recalled as a restorative measure; a digital doppelganger cannot be put back in the box.

Other notions have percolated in the self-regulated environment for informational privacy in the U.S. such as creating a property right in personal information (Lessig 2002; 2006); protecting personal data as intellectual property (Samuelson 2000); and the propertization of a virtual persona as a repository of personal facts (Mell 1996). The property model, though not officially endorsed in the U.S., has nonetheless gained considerable attention as a pro-market based approach to informational privacy as data control. I will explore the electronic persona in more detail in Chapter Three.

In 1967, Alan Westin produced an influential examination of privacy. Westin's formula for fair information practices addressed appropriate collection, use, and dissemination of personal data and his recommendations influenced approaches to informational privacy and data protection in most legislative programmes and self-regulatory schemes in Western liberal democracies. Public and private sector privacy

14 In brief, Prosser (1960, 389) outlined the following four torts: intrusion upon a person's solitude; publicity that painted a person in a "false light;" appropriation of name and likeness for another's advantage; and "public disclosure of embarrassing private facts."

policies and fair information practices or principles (FIPs) have largely been shaped by his analysis and recommendations for balancing intrusive technology against an expectation of privacy. The principles include the issue of consent; defining the purpose and scope of collected information; notifying the public of surveillance; setting up privacy agencies as standards bodies and regulatory watchdogs; penalties for regulation infringement; and instituting freedom of information and data protection statutes (Westin 1967, 367-387).

While Westin's work has had many positive effects it has also privileged the notion of informational privacy over other competing notions of privacy. Other scholars situate privacy as a central pillar in the construction of the ideal liberal individual as either a point of autonomy or one of access (Moore 2003). Joseph Kupfer suggests the "development of the autonomous self" is only made possible through privacy (1987, 81). Jonathan Kahn (2003) argues that privacy allows the autonomous individual to choose when to be private and when to be socially engaged; when to share personal information and when to withhold. Choice is itself affected by factors such as gender, race, and socio-economic status; differently situated individuals are differently able or free to exercise choice.[15]

Kupfer and Kahn's perspectives suggest a space-based concept of privacy or at least a condition of privacy necessary to the constitution of the self; however, within the

---

15 The feminist critique of privacy has illustrated this well. Feminists have pointed out that privacy and the private sphere have been used to protect the most oppressive and cruel inequalities of patriarchal society, however, recently feminist scholars have attempted to re-engage with this debate and re-situate privacy as a space and place for self-reflection and self-development important for defining the gendered subject. See Patricia Boling (1996), Anita Allen (2001), and Jean Cohen (2002). Priscilla Regan makes a useful distinction between choice and consent whereby "choice addresses the rational, economic individual while consent addresses the political, social individual (2003, 15).

network society, the "space of flows" may be dislodging the "space of place" central to the constitution of the self. This tension between a notion of privacy tied to the constitution of the self is exacerbated by a network society in which material, physical private space is more and more infiltrated by persistent monitoring systems. In Canada, the OPC and popular media have also reinforced informational privacy – individuals are encouraged to 'worry' about keeping personal facts private under the auspice of data protection and to 'worry' about what happens to collected personal facts rather than worry about the act of data collection itself (CBC.ca 2005, 2007; OPC 2004).

Identity

Identity in postmodernity is fluid and multiple; the persistent surveillance in the everyday digging up, drawing out, and delivering of personal data into the flows means the natural person can be reconstituted in cyberspace in multiple ways. Poster, in a recent work on identity theft, gracefully lays out the challenge of postmodernity to liberalism's staid, centred self (2007). His explication of identity theft suggests that if liberalism views identity as the basis of subjectivity then identity cannot be stolen like a thing, a piece of property, or a car (2007, 118). Identity becomes/is an object in this rendering.

Poster's earlier work on the notion of the database as discourse (1996) also points out the strain postmodernity places on the liberal self. The prospect of databases as language or discourse is best thought of as a practice operating in the network society in which databases reconfigure the constitution of the subject (Poster 1996, 182). Under this model, the subject is capable of being acted upon by computers and inscribed by facts

captured in the database which operates as a "perfect writing machine" in absence of the natural person (Poster 1996, 184-185).

Detlev Zwick and Nikhilesh Dholakia (2004) extend Poster's databases as discourse thesis to specific instances in the market in which the consumer subject is objectified and acted upon by commercial database technologies. Martin Dodge and Rob Kitchin (2005a, 2005b) do not reference Poster, but arrive at a similar conclusion in the examination of identification codes used to categorize and profile individual subjects; theirs is a detailed breakdown of the workings of systematic encoding that makes data processing possible. The machine codes render the subject as object and the object becomes code in their model. These multi-threaded strands of Poster's original Foucaultian analysis support, I suggest, the notion discussed throughout my thesis – that digital doppelgangers are objects of code and bear the informational hallmarks of identity generating consequential outcomes for the natural person.

Virtual or digital identities are continually reproduced either by individuals themselves through email identifiers, login ID and passwords, online avatars (graphic representations of the self), account profiles, and transaction-oriented activities (such as shopping and web-surfing), or by code that profiles individuals for actuarial and financial analysis, target marketing, and law enforcement and security purposes. The individual can be reconstructed innumerable times from a variety of data sources; each 'profile' takes on a virtual identity given the conditions and parameters of the code deployed to construct it. This fits Roger Clarke's digital persona as "constructed on the basis of accumulations of structured data" (1994).

Clarke's exposition of the digital persona, however, is not argued as a postmodern figure in the context of identity dynamics and multiplicity. Whereas Poster focuses on the productive forces in databases that objectify and produce individuals with dislocated, dispersed identities within cyberspace (1996, 182, 190): the *many* digital personae over the one persona. Where modernity coalesced around the singular, liberal self, postmodernity resists this 'oneness' with many identities reproduced in cyberspace out of a constant and recurrent stream of personal data in the flows.

Surveillance

There is much critical engagement in surveillance studies and sociology, legal studies, political science, geography, media studies and elsewhere on the proliferating aspects of surveillance in society. Digital technologies have enabled innovative means of monitoring populations and individuals alongside increasingly sophisticated techniques for predictive analysis (Gandy 2006) constructing what Lyon describes as an "unregulated means of social classification, of social ordering" or social sorting (2002, 252; see also 2003a). In turn, this has fueled new avenues of expertise in actuarial science, forecasting, risk prediction and marketing analysis across public and private sector organizations. The implications for the network society reside in the application of new surveillance practices and the ubiquitous collection of personal information, which "allows the active sorting, identification, prioritization and tracking of bodies, behaviours and characteristics of subject populations on a continuous, real-time basis" (Graham and Wood 2003, 228; see also Lyon 2002; Gandy 1993).

Lyon defines surveillance as any "collection and processing of personal data" noting

the "most important means of surveillance reside in computer power, which allows collected data to be stored, matched, retrieved, processed, marketed and circulated" (2001, 2). Lyon's definition turns on computing power as a central component of modern, pervasive surveillance. Gilles Deleuze, in two short essays that are but slivers of his life's work, theorized that societies of control characterize this contemporary moment or period in postmodernity (1995). He suggests that society has shifted from Foucault's decentralized and bureaucratic disciplinary society to one of control marked by information technology and computers (Deleuze 1995, 174-178).[16]

Control, in Deleuze's rendering, is expressed as a modulation, an ever-changing language of control composed of codes that permit or deny access to information (1995, 180). Alexander Galloway (2004) seizes Deleuze's model and applies it to the virtual, coded protocols that structure the flows. His unpacking of Deleuze is an exercise in specificity: control is protological. It governs; it rules; it standardizes; it formalizes and structures the network society (Galloway 2004, 5-9). The details Galloway pulls out of the tangle of technical documentation that describe protocol enlivens Deleuze's limited notations on societies of control by fattening up our understanding of control in contemporary digital networks.

I see the concepts of control societies and network societies as linked in spite of Castells' and Deleuze's very different approaches. Deleuze focuses on the apparatus of control found in the codes of networks (and it is this thesis that Galloway builds on), whereas Castells concentrates on the global flows themselves. The distinctions between

16 Poster (2006, 60-63) cautions that if society is shifting from discipline to control, it is not a linear shift; forms of each have historically been present and continue to proliferate.

the two theories are important because Deleuze's definition places codes of control within the means to surveillance. Castells' work provides a background in broad strokes about the dynamics of capital, production, experience and power against which a discussion of identity, privacy, and codes of control can be situated within the network society, but he does not comment in detail about surveillance (1996, 14-18).[17] For the purposes of this project, the network society and flows supply the canvas on which Deleuze's control attributes play out.

Contemporary surveillance scholarship owes much to the work of Deleuze working independently and in partnership with Felix Guattari. Deleuze and Guattari (1987, 4, 7) articulated the concept of "assemblages" as information in the flows collected along "rhizomatic" or root-like tendrils connected to organizations of power and other collectives. The term rhizome conforms to a distributed model of interconnectedness prevalent in information systems theory about branching pathways along a network with interconnecting nodes or junctions; there is no unifying centre in this model and branches disconnect, grow, re-form and reconnect.[18] From the work of Deleuze (1995) and Deleuze and Guattari (1987) surveillance theorists have mapped the relevance of control and assemblages to the proliferation of pervasive computing and surveillance.

Kevin Haggerty and Richard Ericson (2000) refined Deleuze and Guattari's concept of assemblages by developing the notion of the "surveillant assemblage." This is the

---

17 There is a separate critique of new theories of society that could be made in either case over whether societies of control or the network society are anything but a continuation of industrial capitalism. For a scathing critique of Castells see Abell and Reyniers (2000); for a critique of Deleuze see Poster (2006).

18 Galloway (2004) emphasizes distributed networking in his explication of Deleuze's rhizomatic metaphor, however, networking technology in actual application relies on a sophisticated combination of decentralized networking deployed using distributed network management, see also Koch and Westphall (2001). In general, Deleuze and Deleuze and Guattari rely on metaphor that draws heavily on distributed systems theory and complexity science (for language see Power 1990, 1993; and Riva *et al.* 2005; for critique and explication see Mackenzie 2005; and De Landa 2002).

convergence of once discrete surveillance systems into surveillant assemblages that "abstract human bodies from their territorial settings" and separate them into discrete data flows which are reassembled into 'data doubles' for analysis and targeting (Haggerty and Ericson 2000, 606-609).[19] Haggerty and Ericson's surveillant assemblage and constituent data double are together one possible *process* of reproduction. William Bogard has recently theorized that the surveillant assemblage has morphed into the "simulation assemblage" because it is wholly based on computer modelling of the assemblage (2006, 118). I have a different perspective; I propose that the codes of control are implicated in the reproduction of the digital doppelganger regardless of the composition or model of the assemblage itself. This, it seems to me, is not addressed in contemporary surveillance studies.

Oscar Gandy Jr. observed that data processing has become a powerful force for state and corporate bureaucracies whose power has increased through the accumulation of information which, even as governments proclaim decentralization, is actually concentrating centralized authority by extending networks of information and control (1989, 65). This aids the aspirations of neoliberal governmentality to gather more and more data on populations to govern at a distance and in which "Surveillance is 'designed in' to the flows of everyday existence" (Rose 2000, 325; see also 1993).

Greg Elmer's (2004) critical study of consumer surveillance underscores this point. In his study of consumer profiling, Elmer delves deeper into the behaviour of the

---

19 In technical terms, networks and flows are described in graph theory. It is from graph theory that most of us, without realizing it, get the picture of networked connections with 'nodes' as connector points (a line or multiple lines all connected by dots). A network diagram can be a straight line; or, centralized with lines radiating out from the centre; or, honeycombed or lattice-like with no visible centre. For basic explanation and discussion see Barnes and Harary (1983); and Bermond, Delorme and Quisquater (1986).

database systems within technologies of commercial surveillance exposing the binary push/pull between consumer solicitation and response. His work offers an explanation for the operative features of data acquisition (Elmer 2004, 80) relevant to this project's understanding of how data moves between the home and market sphere. He maps the "everyday data economy in which habits, routines, rhythms, and flows are digitized, coded, and diagnosed for the purposes of control" suggesting consumers accept monitoring as a part of ordinary life transactions (Elmer 2004, 42). This behaviour is referred to by Poster as the "interpellation by database" in which the observed become willing participants in such surveillance by providing the information requested during the life transaction (1996, 187). Foucault's panopticon model, which required surveillance to function, also relied on a "network of relations" between hierarchical figures in the disciplinary power structure ([1997] 1995, 176-177), but Poster's interpellation thesis suggests a new "superpanopticon" which leverages the power of databases and can operate productively across multiple networks (Poster 1996, 182-185).

It is this examination of the forces present in the monitoring and collection technologies themselves and their ability to inscribe new identities on the subject as an object of surveillance that is most relevant to my project (Poster 1996; Zwick and Dholakia 2004; Dodge and Kitchin 2005a, 2005b). The doppelganger effect, I propose, is the outcome of such forces.

Code and law

William Mitchell (2003, 189) discusses access control in technologies of surveillance and data collection and describes them as "logic prisons." His discussion is

part of a broad synthesis of the influence of technology on social change, but it maps to this project by setting up a rather apropos metaphor for interrogating the network society's codes of control. Database management systems (DBMS) are one possible "logic prison" and provide codes of control to organize meta-data (data about the data) and databases. The systems incorporate a suite of applications, or component elements, that make data processing possible and include: the database(s), the collection and storage rules, the interoperability modules, analysis engine (predictive analysis capabilities, sorting and profiling functions), communications rules, access codes, archival-retrieval system, and all the object-relational aspects (Power 1990; Hernandez 2003; Powell 2006). This multidimensional code set figures prominently in the doppelganger effect by enabling the analysis and productive techniques of profiling and identity reproduction to which I will turn in Chapter Four.

Code and issues of control, however, worries the law. Lawrence Lessig is probably one of the most prolific legal scholars taking up the challenge of regulation and control in cyberspace with an eye on the code (2001; 2004; 2006). His work has examined the tensions between content creators, consumers and private corporations as owners of digital media, and between information access and corporate governors of access control. Lessig proposes that the technical structure of cyberspace, Galloway's protocols, are a key element upon which legal instruments that offer material support and legitimacy for regulatory regimes in cyberspace are built: "code is law" (Lessig 2006, 5). Lessig sees code as a regulator and in cyberspace regulation operationalized in the codes of protocol controls things, people, activities, and information.

Other legal scholars have also grappled with regulation governing information in cyberspace with varying levels of specificity. Dan Burk (2003) examines the coded constraints built into DRM that limit unrestricted access to digital content. Craig McTaggart (2003), in a well-balanced explication of the coded, layered architecture of the Internet, suggests that the structure of the Internet itself could map to specific regulatory instruments as a guideline for policy development.

There are, however, many weaknesses in relying on 'code as law" which this literature does not identify, not the least of which is the challenge to its stable character posed by poststructuralist interrogations found in the work of Poster (1995), Dodge and Kitchin (2005a), and Zwick and Dholakia (2004). The logic of protocol with its rational, coded structure aligns nicely with rational, codified, procedural and regulatory laws, but as I hope to demonstrate in Chapter Five, things are not always what they seem in cyberspace and, as a result, laws might not mean much to the digital doppelganger.

The code or software that constitute databases are the real lynchpin in the flows and for the network society the "new power lies in the codes of information" (Castells 1997, 359). It is the productive power of this code, the code that *captures*, that *analyzes*, that *transforms*, and *machines* raw data into a sleek cube of information that generates the doppelganger effect in the network society.

Complex effects

In the opening sequence of this introduction, I invoked the metaphor of chaos theory's butterfly effect. The butterfly effect posits that the most subtle change in a nonlinear system will effect monumental change over time due to a sensitivity in initial

conditions within the system (Lorenz 1963; Ditto 1995; Bradley 2007). It became part of popular imagination when it was invoked by Edward Lorenz to explain how the flapping of a butterfly's wings could alter the initial conditions of a weather system and result in a tornado (1963).[20]

It is not my intention to use complexity science as a rhetorical tool to unnecessarily complicate my own analysis of code, home spaces, network flows, and identity. I am not attempting flight, as it were, along the obscure path of butterflies to make a point simply about the unanticipated consequences of code. Chaos theory demonstrates that when existing structures and behaviour in systems of relationships change over time, the changes are amplified in unanticipated ways creating unexpected outcomes and while such changes may seem random and chaotic they in fact occur within defined mathematical parameters (Kiel and Elliot 1996, 4,5). The doppelganger effect is only a neat little capture point, borrowed from the effective analogy of the butterfly effect, to illustrate the power of flows and the productive power of code; power that can shift in radical ways with the slightest nudge from a misdirected byte in the data stream yet still be organized by the code that defines it.

I am aware of the tensions between those who deploy complexity science metaphors in social theory and those in the scientific community who deplore their use (DeLanda 2002; Mackenzie 2005);[21] however, chaos theory itself is studied in relation to

---

20 Lorenz, in the early 1960s, originally studied the effect of chaos in weather systems which are notoriously difficult to predict (1963).

21 There has been tension between the hard science fields and social theory and the use of complexity science metaphor exemplified by the Sokal Hoax in which Alan Sokal (1996) published an article full of invented theory and analysis as harsh criticism of the use by scholars such as Deleuze and Guattari, Lacan, Kristeva, and Irigiray of complex scientific terms to describe the postmodern condition. Sokal describes the experience and expands his attack on social theory in *Fashionable Nonsense* (Sokal and Bricmont 1998).

information systems because of that system's inherently unpredictable response to change which figures in all complex distributed systems (Dhillon and Ward 2002; Power 1990, 1-2; Ditto 1995, 98). Distributed systems underpin the complex network of intelligent systems and embedded technology and communications within surveillance technology and data processing (Steventon and Wright 2006). The complex interconnections between and among codes of control are what power the rhizomatic undergrowth of Deleuze's societies of control. Distributed systems make the network society function as it does and forms the basis of Galloway's (2004) protocol thesis and Castells' information flows as the framework for an adaptive, flexible network.

Methodology

My thesis proposes a new theory to explain the reproduction of identity out of the facts and minutiae of private life collected by monitoring systems embedded in the everyday. The doppelganger effect is in a constant and productive state of becoming; it is iterative and builds upon itself sensitive to minor perturbations generated by ever-increasing sources of personal data. As the preceding discussion outlined, this thesis takes as one of its theoretical starting points Poster's (1996) poststructuralist model of databases as discourse. This idea is central to my exposition of the flows of code and the code of flows as productive forces capable of generating the doppelganger effect. An effect that gains form in the network society from Castells' parallel notion that "the power of flows takes precedence over the flows of power" (1996,469).

One of the central challenges for my thesis is to map out the traces and effects and the places and spaces in which the doppelganger effect emerges. To demonstrate my

theory, I develop a schema of interconnected concepts and phenomena that will expose the traces of the individual caught up in the information flows of the network society. This schema captures places, spaces, personae, databases and governing structures in its net constructing a map of relations to illuminate how the consequential outcomes of "perfect writing machines" come to bear on the individual. My schematic approach thus serves as a framework to organize chapters around the corresponding phase of the data cycle, namely, collection-analysis-dispersal, and finally the laws and regulations governing data collection, use and disclosure.

The preceding literature review locates my object of study, the doppelganger effect, across multi-disciplinary scholarship. I examined secondary sources in surveillance studies, sociology, media and cultural studies, law and privacy, computer science and technology, and systems engineering. Each of these diverse fields lends something to the thesis schema to lend shape and form to the spaces and places and traces and effects I will expose in the forthcoming chapters.

To demystify the complex aspects of distributed computing and pervasive systems central to my thesis I have analyzed systems engineering sources extensively. While sociological material commenting on the network society and Deleuze's societies of control provide rich avenues to explore the social and phenomenological aspects of my proposal for the doppelganger effect, complexity science and engineering help to anchor my understanding of the technological innovations and constraints relevant to the network society's distributed network. I pay particular attention in my research to the conceptual framework in science and technology describing future pervasive systems and

distributed computing to balance the rush to analyze these complex proposals for the future in contemporary sociological literature addressing the 'smart home' in often vague terms.

My references to database technology throughout the thesis have combined my previous training and study in digital technologies with recent technical developments in the area of databases giving me confidence in tying the operative characteristics of the doppelganger effect to proposals for the productive power of code and databases. There is a case to be made, as I hope to demonstrate in my thesis, that databases and the analytical capabilities engineered into their inferencing engine are getting 'smarter' and productive.

I will incorporate several examples and anecdotes at different points in my thesis to illustrate the doppelganger effect. I selected two examples of data breaches, one from the private sector and one from the public sector, which exposed personal information. I selected these as illustrations of the type and quality of information collected and retained by organizations. The first of these is the TJX Corporation data breach which involved the theft of millions of customer records comprised of personal information such as driver's license, credit card details, and name and address (TJX.com 2007).

The second example from the public sector occurred when Her Majesty's Revenue and Customs Services in the United Kingdom (HMRC) lost a set of disks containing millions of citizen records consisting of personal information such as national insurance number; name, address and birth date; spousal details; names, sex and age of children; and bank account details (BBC.co.uk 2007).

I chose a third example involving a public figure, Kobe Bryant, and a private individual misidentified as the victim of his alleged sexual assault. The details of this case of mistaken identity and reputation circulated on the Internet amplified by the indexing and cataloging features embedded in search engine databases. I will use this example to highlight the productive power of code implicated in the doppelganger effect.

I did not conduct formal interviews or empirical analyses for my thesis. I relate unsolicited anecdotal stories which were revealed in conversation directly to me as well as my own experience of being profiled for an insurance claim. The two anecdotes relate to specific instances of profiling which resulted in unexpected outcomes for the individuals involved, sharpening the distinction between identity in the material world versus the identity reproduced and assembled by databases in cyberspace.

The first element in my schema appears in Chapter Two where I begin my analysis of the constellation of effects implicated in the doppelganger effect. Here I will examine spaces and places and the notion of the 'smart home' and its embedded codes of control within pervasive systems. In Chapter Three I expose how and where the traces of the natural person are theorized to reappear in the analytical outputs of database systems.

Chapter Four will theorize on the doppelganger effect in an explication of the consequential outcomes of "perfect writing machines" or databases. I will incorporate the aforementioned examples to augment my theory of the doppelganger effect. My thesis will conclude with a critique of the approach to informational privacy and data protection common to most Western liberal democracies. The doppelganger effect poses a challenge

to conventional laws and regulations governing cyberspace, not the least of which is the way the individual is reproduced from the facts and details of private life.

I begin my analysis in Chapter Two by focusing on data collection in the home.

Chapter Two

Spaces and Places: Privacy matters and matters in private

> A whole history remains to be written of *spaces*... from the great strategies of geo-politics to the little tactics of the habitat.[22]

In "Power/Knowledge" (1980) Michel Foucault suggested that the "little tactics of the habitat" and "politics of space" have suffered a long neglect in history. Foucault's work linked the evolution of architecture and populations to the emergence of the home at the end of the nineteenth century as a differentiated space with specific and functional spaces within it. Foucault also wrote that surveillance of individuals and spaces is a form of power "applicable to many domains ... 'power through transparency,' [and] subjection by illumination'" (1980, 154). His exhortation seems a fitting starting point for this chapter's focus on home spaces, privacy and surveillance in the domestic sphere.

Foucault's reference to power reveals a subtext in the ongoing tension outlined in Chapter One between space of places and space of flows. This subtext can be read in part as the neoliberalization of the domestic sphere whereby forms of self-surveillance and passive monitoring in the home fulfill the goals of a self-disciplining apparatus essential to neoliberal forms of governance (Hay 2000). The fulfillment of this objective, I argue, requires the home to be connected to networks, to the flows, and constantly monitored while at the same time effecting a sensation of privacy and self-direction for the individual.

In addition to the social and political aspects of neoliberalism that I argue contribute to the transformation of domestic space, other factors alter the home space. In this

---

22 Foucault (1980,149).

chapter, I will also examine the interactions between the individual, home spaces, and software suggesting these have a transformative effect on the spatial reality and form of the home. To illustrate this I will explore the 'smart home' concept with its embedded codes of control that coordinate a multitude of systems within the home. Several corporations and institutions have embarked on research projects involving smart home pervasive systems including Microsoft Corporation and the Massachusetts Institute of Technology (MIT).[23]

The pervasive systems of the smart home require ongoing data collection to function and localized network functionality to communicate as well as routine connection and transmission of personal data from home system to corporate system to function. An example of how data collection and transmission will (and does) operate can best be illustrated in the example of copy protection systems on personal digital devices such as the computer. Persistent monitoring present in technology protection measures (TPMs), specifically digital rights management systems (DRM), match a licensed user to the corporate license database of the content provider.[24] This is a useful illumination of the data cycle at work in embedded systems in/of the home and particularly significant for smart home development as PICT research cites DRM as a successful model and strategy to follow for pervasive systems in/of the home (Bull, Limb and Payne 2006).

The self-governing habitat

In Western affluent nations of the twenty-first century the domestic sphere is

---

23 There are other pervasive computing and 'smart home' concepts being researched including IBM's 'Smart Kitchen' (ibm.com); Xerox's PARC studies on ubiquitous computing (parc.com); and HP's CoolTown research (currently on hiatus it appears; cooltownstudios.com).

24 DRM and other TPMs operate on a wide range of mobile handheld devices such as iPods and cell phones as well as laptop computers but its entrenchment on digital devices in the home is relevant to this chapter's discussion of smart home systems.

comprised of fully integrated spaces in which interconnection, integration and multifunction dominate how individuals interact in the home mediated by sophisticated digital technologies. Technology in the home, whether ICTs or utilities, television or telephones, places the home within reach of the market sphere by allowing corporate capital to collect and disperse private facts into the commodity sphere.

As the home became more privatized throughout the twentieth century, broadcast media technologies and utilities provisioning (electricity, gas, and oil) connected homes to a grid and flows of information, goods and services. Raymond Williams' ([1974] 1990) notion of "mobile privatization" provides an account of emerging regimes of mobility and privacy wherein individuals lived further away from work and government. Television, in this model, became vital in reproducing and maintaining cultural and social practices that brought the market sphere into the private domain (Hay 2000). This, I would argue, folded the home into an evolving neoliberal economic and governmental practice engineered toward inducing a complex set of self-governing actions undertaken by individuals in the home to reproduce desired social goals. As James Hay proposes, neoliberal governmentality has transformative capacity and the emergence of the "self-governing household" is under the coordination of state power but "operate[s] outside its direct control" (2000, 69).[25]

Neoliberal governmentality requires data on populations to function using "operable technical forms for exercising perpetual scrutiny" to govern "spatially and

25 Of course these self-governing actions are not reserved for the domestic sphere. See Thomas C. Patterson (2005, 373-380) for a broad accounting of neoliberal governmentality and Nikolas Rose (2000) for a discussion of neoliberalism and its relationship to power and control directed toward targeted populations. There is a notable quote from Margaret Thatcher (1987) that sharply outlines advanced liberal/neoliberal views of populations: "There is no such thing [as society]! There are individual men and women and there are families" (margaretthatcher.org).

constitutionally – at a distance" (Rose 1993, 13, 10). One such "operable technical form" is surveillance technologies. The rationalizing tendencies of bureaucratic systems coupled with the notion of cheap, private sector social control in which individuals actively participate in their own surveillance by interacting with the technologies as a matter of modern life ensures a steady stream of personal and other data (Gandy 1989). The rhizomes of control extend out along "new vectors of responsibility and obligation" instrumentalized through the "regulated and accountable choices of autonomous agents" (Rose 1993, 16).

The classic liberal individual remains at the root of the rhetoric spun out by neoliberal governments; the individual as an autonomous, self-directing person. However, as neoliberal instruments of control propagate through technologies embedded in the everyday/everywhere the individual central to their mode of governing is slowly being destabilized by the codes that collect, reproduce and profile the individual subject. The liberal individual is thus more and more fragmented in cyberspace displacing "essentialist and unified notions of 'the individual'" (Dunn 2000, 119) central to liberalism's governing objectives.

What I am arguing here is that as the home is captured in an extended, rhizomatic net, it is subsumed by domestic monitoring systems that blur the boundary between private domain and market sphere. Neoliberalism treats the market unproblematically such that an individual's actions are seen only as rational choices to satisfy needs and desires through consumption (Patterson 2005, 377). Neoliberalism and its emphasis on individualism and self-responsibility pushes the home to the edge of the flows and, I

argue, permits its market-based focus to permeate the home via ICTs.

Spaces and places

In this contemporary moment smart technologies in/of the home have become bound up in an often subtle interplay between individuals, space, and code. This trio of forces arguably propel the individual into choices that trade connectivity to the flows of the network society for increased monitoring in the home. From the simple act of switching on a light in the bedroom to punching in the key code on a home alarm system, individuals are continually monitored in places once assumed to be free of surveillance. The data collected carries a mélange of personally-identifiable details and facts and personality-based behaviours and preferences, a veritable snapshot of routine habits of the individual in private life.

In their analysis of code and space, Martin Dodge and Rob Kitchin (2005a) trace the everyday routine encounters between people and software (code). Their work uncovers the "effects of software (code) on the spatial formation of everyday life" emphasizing the productive power of code, or 'technicity,' that mediates routine encounters between individuals and their environment (2005a, 169).[26] Technicity is, in their application, the overall productivity in and of technology to make things happen akin to the notion of the "productive power of databases" (Zwick and Dholakia 2004). The process describes an iterative spatial formation; a progression of shape-making and meaning-making emerging

26 Adrian Mackenzie also draws on the work of Gilbert Simondon's notion of 'technicity' described as a "network of relations" and "a unity of becoming"within technical ensembles (as cited in Mackenzie 2002, 14). In the context of my thesis, home spaces, embedded systems, and digital devices would constitute part of a technical ensemble along with the communications infrastructure and networks required to collect and disperse data; Alain Pottage defines "techne" (historically associated with legal rhetoric) as a mode of production that has "power or capacity to produce things whose eventual existence was contingent upon the exercise of that power"(2002, 275).

out of the "conjunction between code and people" (Dodge and Kitchin 2005a, 178; see also Mackenzie 2002). This is one possible way to interrogate how the space of place transforms to become a space of flows. Code and individuals mix to reformulate how space is used, altered and made anew in the home. Territories, such as domestic space, once distant from or only partially connected to flows of goods and services, commerce and global capital are now re-mapped as part of the flows.

The home, then, is not a passive space but relational and in a constant process of reformulation based on socio-spatial relations; it is a "practice, a doing ... a material and social reality forever (re)created in the moment" (Dodge and Kitchin 2005a, 171-172). In the context of the home, code (software) modulates, mediates, communicates, and regulates against a panoply of social and spatial distributions. Shortly I will turn to a fuller discussion of the smart home in which code is embedded into its literal frame making the modulations and mediations evident in a material way.

Lieven de Cauter has suggested the home is becoming capsular; " a plugged-in terminal" on the network and "a closed-off and plugged-in entity" (2004, 96). However, this conveys the notion of the home as an end point in which capsularization increases as network connectivity intensifies, whereas, I am arguing instead that the home is a nodal point on and within a vast network permeated by data moving bi-directionally from and to the flows. The notion of individuals enclosed in a capsule riding out the storm of information flows belies the complexity of the network society. The home, I argue, has become one of many spaces connecting to/with the flows at once seemingly physically private and yet exposed to global pathways of information. It cannot be effectively

encapsulated. There are no end points in the distributed network infrastructure of the network society; there are just rhizomatic tendrils which extend in every direction collecting more and more entities.

de Cauter's comments project the notion that individuals can be contained within a sort of material or virtual bubble which both mediates or mitigates reception and experience of the network. It insulates the individual against the risks and pressures of an external world of virtual flows and material dangers. He posits that the home can be walled off *at the same time* as it is plugged-in to the flows (2004, 96). I challenge his capsularisation thesis because the previous materialist notion of fixed boundaries and impermeable walls cannot be sustained. Explicit technologies used to 'firewall' a home and construct a protected boundary through mechanized and digitized security systems or computerized anti-virus programs each require two-way communication in and through the flows. The home as a coded space suggests that there is nothing static about it. There is no 'walling off' of spaces because the space itself is constantly made and re-made as individuals interact with the code (software) in it.

The neoliberal emphasis on the self-responsible individual drives the need for systems that enhance and reinforce a sensation of control over one's environment and experience. I disagree, however, that it is the capsule that insulates the individual against the raw force of the network society. The interface or connection to the flows, I argue, occurs directly between the individual and the flows; a more cybernetic interlocution in which the individual can be anywhere and interface with the network. Devices through which the individual communicates and interacts with cyberspace do not act as a buffer.

There is no capsule, only the individual.

de Cauter's remarks were in response to Manuel Castells' notion that the space of flows is overtaking the space of place as the dominant logic of the network society (Castells 2004, 85; de Cauter 2004, 96). I do not suggest an abrupt shift from one spatial configuration to the other is occurring, but that the space of flows has ruptured the sense of place integral to privacy. The home remains a physical construct in a defined geographic locale and hence a 'place,' but it has become a liminal space: it occupies and is occupied by both spatial realities, flows and place. In concert with other forces examined here there is a transmogrification of the home underway which destabilizes assumed states of privacy within the home.

Individualized experience heightens feelings of control and self-expression in and over one's domain and yet many of the required actions for self-control over the home environment expose private tactics, activities, choices, and preferences. The home feels like a separate place removed from, or separate from 'out there' and distant from other virtual spaces, and yet the technologies that deliver this feeling of solitude, security, privacy, and individual choice subtly yet effectively expose the nuanced actions of personal, even intimate, life choices.

The smart home

Domestic intelligence

Theodor Adorno envisioned the modern home as "living-cases manufactured by experts for philistines, or factory sties that have strayed into the consumption sphere" (Adorno [1974] 2005, s.18). His is an especially bleak vision of the modern home

infiltrated and corrupted by commodification, but is he wrong? Microsoft Corporation proposes their home of the future will make "daily activities more enjoyable, efficient and productive" by providing *consumers* with products and services to enhance their life (Microsoft.com 2006). The Microsoft Home will require that consumers and businesses tie themselves to Microsoft products adept at facilitating network communications with market services from the local grocery store and pizza restaurant to copyright-enabled entertainment content (Heath and Bell 2006).

One of the central concepts of the smart home is its 'intelligence.' In Hay's analysis of the "new mobile privatization" he defines this 'intelligence' as a "regimen of applications and a rationality/science of home management" directed toward achieving "domestic freedoms" (2006, 367). The "regimen of applications" in the smart home enable interconnectivity and efficiency, self-regulation and self-reliance, through wholly sentient spaces merging once separate inside/outside and work/home distinctions (Morley 2003; Spigel 2001). This transformation, I suggest, is important to the reorganization of home space from a private place to one of a space of flows allowing multiple and concurrent personal and work experiences to occur in one's living space.

The Microsoft Home emphasizes 'intelligent' media delivery systems and environmental controls consolidated in a handheld device such as a "mobile phone to control room lighting, temperature, music, television and other parts of the house (Bishop 2006). Though this and Microsoft's vision of a teenager's bedroom with surface computing turning walls into interactive media spaces replete with customizable sound

and images is intriguing, the reality will be difficult to create.[27] The Microsoft Home is built around proprietary Microsoft technology and media systems which are not designed to work seamlessly with other smart home vendors (Heath and Bell 2006). If the smart home of the future hosts a "regimen of applications" to enable smart living then interoperability and integration will become critical in bringing the Microsoft Home to life.

The smart home is being designed explicitly to contain an "information layer that supports a reasoning ability – sometimes referred to as ambient intelligence" (Bull, Limb and Payne 2006, 83). This awareness or sentience in/of the home space requires data flows to function and to communicate with other objects and systems on the network. These localized flows are coordinated within the home but require connections to external corporate host systems that provision content, servicing, product and system updates, and security monitoring.[28] The "information layer" engineered into the smart home creates fully "informationalized space" in/of the smart home which in turn creates new objects of analysis (Thrift and French 2002, 325). These new objects of analysis distill from personality-based data gathered by smart systems and generate new kinds and types of knowledge about the individual in private life.

Pervasive ICT (PICT) systems are intended to have four autonomic or self-managing properties: be self-configuring; self optimising; self-protecting; and self-

---

27 The Microsoft Home has been around for over a decade and has not changed all that much since I first saw it in the mid-1990s. The current incarnation makes its home in Redmond, WA at the Microsoft campus, but also travels to trade shows and conferences to showcase Microsoft's "latest" vision for the future home. It made an appearance at the 29th International Conference of Data Protection and Privacy Commissioners in Montreal, Canada, September 25-28, 2007.

28 By 2020 it is estimated there will be a trillion communicative objects with information gathering capabilities and connection to the Internet (Wright and Steventon 2006, 2).

healing (Shackelton *et al.* 2006, 323). The purpose, according to research, of such "ambient intelligence" embedded in PICT environments is intended to make the individual user less aware of the technology and its more complex features, even as the pervasive system itself becomes more aware of the individual user (Riva *et al.* 2005). Self-managing faculties always propagate the fittest or most robust network links and decision-making routines in the pervasive system and 'evolve', or 'learn', based on a catalogue of 'experiences' that shape future system 'behaviour' and responses (Rogers 2006). This nomenclature is a strange mimesis: nature reorganized in a parallel universe that reflects Darwin's evolutionary model of the survival of the fittest coupled to the ideology of neoliberal self-actualization.

Posthuman domesticity[29]

The emphasis on sophisticated embedded systems in/of the smart home orients the subject toward the flows and the market as a data object to be managed by pervasive systems: "In the smart house, things relate to things" (Spigel 2005, 411). Spigel views this domestic amalgamation of "silicon and flesh" as a new form of subjectivity she labels "posthuman domesticity." In this modality, the house has become more human through its construction as a smart, intelligent and sentient space while humans have become more 'machinic' and integrated within this "system of objects" (Spigel 2005, 411).

Pervasive systems in the smart home of MIT's vision, called PlaceLab, are more aptly thought of as *persuasive* systems that impart a particular kind of 'smart living'

29 Spigel 2005.

suitable for the smart individual. This entails not simply embedded and easily accessed entertainment and security systems, but more overt lifestyle guidance that encourages a certain kind of behaviour or direct action on the part of the individual. In the PlaceLab one area of research focuses on "persuasive user interfaces for motivating healthy behaviors" to provide 'just-in-time' information about "what people are doing ... in order to motivate behavior change" (architecture.mit.edu). This will require an intense level of monitoring, reporting, analysis, network transmission and communication both within the home and to systems beyond it.

While not as overtly tied to the consumption sphere as Microsoft, MIT's House_n project nonetheless incorporates private sector technology alongside publicly funded academic research into future living and smart homes. MIT aims to "satisfy the emerging and *future needs* of people" to allow people to "maintain *autonomy* as we age" (architecture.mit.edu; emphasis added). This statement implies that the sentient home space will so successfully learn about the occupants that it will predict requirements for the future yet somehow accommodate individual self-determination. In the words of Stephen Intille, one of the lead researchers of House_n, the goal is to "empower people with information to make decisions" not take away control and place it in a pervasive system (2002, 77). I argue that pervasive systems coerce a particular action; that code can be designed to steer individuals toward predetermined social outcomes hinted at in the first quotation.

PICTs will monitor unique, personality-based behaviours reflecting individual choices and responses within the home and recommend action. Whether it is a home

appliance networked to the corporate service centre or a pill bottle with a radio frequency identification (RFID) tag transmitting re-order information to a pharmacy, pervasive systems are structured to communicate private facts from within the domestic sphere out to the flows. What places in the future home are left unexposed? One of the central concerns in pervasive systems research is that privacy is complex and difficult to secure (Bull, Limb and Payne 2006; Rogers 2006). Systems that inherently demand networked communication to function including version updates, bug fixes, and user input are engineered to pass data within and beyond the local network.

Autonomy seems to be the watchword of pervasive systems research. The 'smart home' is not just about making private life easier, it represents what I touched on earlier through Rose's observation that control under advanced liberal economies is expressed through autonomous agents (1993, 16). The kind of smart home envisioned for the future will emphasize autonomy, security, self-responsibility, and I think ironically, privacy. Autonomy in this model is exercised within a narrow range of coerced behaviours directed toward shaping a certain kind of self-reliant individual essential to decentralized modes of governance.

Autonomy, as I will illustrate in Chapter Five, is also central in the data protection and informational privacy approach. As the technologies of the smart home nudge the home space more fully toward a space of flows it is likely that informational privacy strategies will be deployed more explicitly to govern specific pervasive systems data collection practices. It is less likely, however, that information policy will address or in any way limit the surveillance capabilities that will surely reside in home-based PICTs.

This smart home environment is contingent and perpetually forming and re-forming through coded practices between the individual and domestic space. Software in this rendering is an instrument of Deleuze's societies of control operating as a "set of modulations that direct how citizens act" (Thrift and French 2002, 326). An encoding/decoding practice of governmentality, but one in which the actual physical place and space of home is morphing into a 'habitat node' responding to requests for information to and from the flows of the network society. The smart house, then, is "a mode of living situated wholly within the the space of flows" in the service of "diffuse and intricate mechanisms of control and surveillance" (Allon 2004, 255). It is as if "the price of bourgeois utopia is privacy itself" (Critical Art Ensemble 2008).

Copy protection and digital rights management

Specific codes of control within embedded systems built into the smart home, in security systems, computing systems, DVRs, cell phones and other digital devices troll through every input command, keystroke, voice entry, and web click, logging each literal bit of data. It is not simply that embedded systems in the smart home track these actions but that each interaction is potentially reportable as data in an ongoing communication cycle between corporate software or digital media (content) providers and the consumer. This is nowhere better illustrated than in the mechanisms deployed by content providers to monitor their product or digital content and use patterns on computers, cell phones, and digital TV.

An example of 'privatized surveillance' in the home are copy protection systems or technological protection measures (TPMs). TPMs are intended to promote the authorized

use of digital media and technology on personal digital devices such as computers (Feigenbaum *et al.* 2001).[30] In my thesis, I am not analyzing TPMs through the copyright lens which is a common entry point for legal analysis of the privacy and surveillance aspects of copy protection (see Kerr 2005; Cohen 2003). My perspective here rests on the specific capability to return personality-based data to the flows by monitoring media consumption, production and activities that reveal private preferences and behaviours. Thus, I am sensitive to the tightly coupled relationship between content protection through various technical measures enacted by rights-holders and freedom of use by consumers, but view TPMs as but one of a broad implantation of monitoring systems in the smart home. The way corporate rights-holders deploy TPMs and design in the monitoring and reporting functionality is and will be considered as a model for pervasive system developers developing the smart home (Bull, Limb and Payne 2006; see also Dodge and Kitchin 2005b).

Often TPMs are tied to digital rights management systems (DRM) which compel consumers to agree to a set of terms and conditions of use (a usage policy) for the digital content (Feigenbaum *et al.* 2001; Kerr 2005). DRM is a more productive approach for monitoring than TPMs. It requires underlying technical measures to force compliance with legal rules bound together through commercial transactions involving licensed content such as music or video in 'for fee' downloads.[31] DRM consists of six parts:

---

30 In the instance of DVD regional coding the computer or DVD player does not require internet connectivity. The copy protection region code is embedded in the computer or player with a matching component code in the DVD and will effectively block unlicensed use (Acquisti 2004, 8; Stefik 2007, 2). Device and content manufacturers deploy this tactic to comply with product licensing and regional distribution regulations. Most computer systems will allow a regional change three to five times to accommodate 'out of region' content but after that the DVD play capabilities are permanently disabled in the computer (in some cases this can be disabled but it is illegal to do so).

31 Central to the notion of DRM and most file-based protection systems that collect data is consent (Cameron 2004).

content; cryptographic protection; rights expression language (REL); license management (implements encryption key and rights); compliance regulation (device or software that recognizes the license); and client-side enforcement (ensures purchaser complies with the license) (W. Jonker 2007, 259-260). It operates under client-server architecture meaning a corporate-side server (computer) sends the content at the request of the customer, or client-side computer, over a network (most often the Internet). A corporate database operates on the server side to store and track licenses, individual usage, and personally-identifiable data such as Internet Protocol (IP) address (W. Jonker 2007).[32]

The part of DRM that exposes user behaviours and actions is nested under the client-side enforcement element. This is the most vulnerable aspect for the rights-holder as well because it is here that users can attempt to circumvent the copy protection scheme.[33] Of most concern in my thesis are the tracking and reporting features in DRM that facilitate the collection and dispersal of personality-based data – personally-identifiable data combined with use patterns that reflect individual preferences.

DRM monitors and controls user activities tracking what is read, watched, and listened to at home and relays the information back to the corporate rights-holders.[34] It offers a peek into private life not previously observed by either the state or private sector

---

In this chapter my discussion focuses on the collection and dissemination of the data and in Chapter Five I will specifically address consent as part of the approach to data protection and informational privacy.

32 Apple Corporation embeds account data in its proprietary music files – even those that are free of licenses or explicit DRM (ars technica 2007).

33 Circumventing copy protection is illegal in many jurisdictions including the USA which has the *Digital Millenium Copyright Act* (DMCA) and makes it illegal to tamper with copy protection. Canada is pondering its own version of anti-tampering provisions within a revised copyright Bill yet to go before Parliament as of February 2008. See Prof. Michael Geist's blog, michaelgeist.ca and faircopyright.ca for current and past debates on Canadian copyright issues.

34 The best known DRM systems include Apple Corporation's FairPlay (one of the most sophisticated and onerous; see Apple.com); Microsoft DRM (microsoft.com); Open Mobile Alliance for protecting content in wireless applications and scenarios (openmobilealliance.org); and Marlin for sharing content across multiple devices in a home network (marlin-community.com).

corporations through other consumptive acts. DRM kicks in after the purchase of digital content; however, unlike the purchase of a paperback book where no further data becomes available as to how, when and where it is consumed, copied or passed on, the digital DRM-enabled content is forever monitored (Kerr and Bailey 2004). There is a clear case to be made here that DRM seriously limits freedom of expression, a concern taken up by Ian Kerr and Jane Bailey in which they discuss the "unprecedented degree of surveillance" enabled by DRM systems (2004, 89). They suggest a rather more obvious label for DRM as "digital rights monitoring systems."

After product installation, which often requires an alpha-numeric license key to verify proof of purchase and enable access, a DRM embeds in the operating system of the digital device (W. Jonker 2007). No user intervention/interaction is normally required post-installation and the DRM transmits every discrete action involving the protected content back to the rights holder ostensibly as part of the license matching and authorization process (CIPPIC 2007; Subramanya and Yi 2006). It is here at the system level that DRM diverges from other more obvious transaction-oriented data collection systems individuals encounter in the public and market sphere which involve direct action by the consumer.

Surveillance technologies present in DRM systems and their institutionalization by private sector companies as a mechanism for enforcing copyright have given corporations and content providers, as rights-holders, unprecedented control over private choices and actions. Private sector firms now have one of the most potent tools for social control to regulate private conduct embedded in widely disseminated technology and digital content

(Kerr 2005; Kerr and Bailey 2004). Following Gandy and Rose's explication of the instrumental nature of monitoring to induce certain behaviours, it seems likely that such technologies of surveillance and control common to modernity force individuals to alter their behaviour. Individuals regulate their own conduct and internalize the 'correct' behaviour because they know they are being observed (Schoeman 1992, 118-119).

Private matters

Although social control and freedom of expression are important aspects of the debate surrounding DRM, my thesis is interested in its role in exposing private life choices and actions. In particular, I am suggesting that DRM is a good illustration of how pervasive systems (always on, always enabled) will persistently connect to corporate databases. The notion of persistence is important not just to iSpaces and ambient spatial technologies but to content-based monitoring systems such as DRM. In computer parlance a 'persistent state' requires the system to track and 'remember' certain events, chronologies, or actions linked to a unique file (Shapiro and Vingralek 2002). Persistent data in a DRM system might include logging file access for listening or viewing purposes and/or file copying to make backups or share with others.

In addition to the persistent state information captured and communicated by the DRM system the digital file itself may have 'secret' embedded properties to identify both the copyright holder and user. This may be done through 'fingerprinting' or 'watermarking' to encode the file with copyright information and is often coupled to a trace feature attached to the file identifying the user (Feigenbaum *et al.* 2001; Jonker *et al.* 2004). In the case of 'pirated' content the trace feature enables the copyright holder to

identify a user who purchased the content and released it "into the wild" (Jonker *et al.* 2004, 5).

Research into both DRM persistence and pervasive computing systems is focused on security. The emphasis on security is one-sided. In DRM systems security is targeted at protecting the digital content from attempts to tamper with the copy protection scheme and at protecting the log files that contain personal use data collected by the DRM system and sent to the corporate database (Shapiro and Vingralek 2002, 184). Very little emphasis is on securing the user's privacy or protecting their identity (Cameron 2004).

In pervasive systems, such as those in the smart home, a level of openness is required to facilitate the communication between heterogeneous network elements such as household appliances, room controls, computers and entertainment systems. Research and development into pervasive systems acknowledges that seemingly trivial information will be gathered by these systems but it is "personally sensitive or commercially valuable when correlated with other ... sources" (Wright and Steventon 2006, 14).

If privacy-enhancement is not explicitly designed into the systems of the smart home then the focus will remain on security which is inherently hierarchical and structured around access/denial of access organized by codes of control. By its very nature this binary system requires communication between entities on a network: client-server, user-rights holder, and consumer-distributor. Matters in private, the "little tactics of the habitat," are thus transported from the private sphere to the market sphere in an endless cycle of commercial negotiation and authorization between private system of reception and corporate system of production and control.

Conclusion

A theme that surfaces often in smart home discourse is that of the interface between human and 'machine' or cybernetic humans. Nigel Thrift and Shaun French suggest that software is "part of the extended organism of a new form of humanity" wherein software is "building using writing" (2002, 329). This is also reflected in Spigel's notion of "posthuman domesticity" and certainly in Poster's database as discourse theme to which I will return often in this thesis in relation to the doppelganger effect.

The human/machine discourse ties together notions of effectivity and productivity of code/software in the smart home to the spatial transformation evolving out of the multiple ways individuals interact within this digitized environment. New modes of subjectivity, regardless of the descriptive term used, acknowledges, I think, that new forms of space come into being alongside the interlocution of individuals and code. This becomes integral to the argument that the space of place can be and is being morphed into a space that ensures seamless connection within the network society – the space of flows. The condition of privacy experienced as a spatial phenomenon free from observation and monitoring is virtually impossible in this scenario.

If data collection by DRM systems, and other systems embedded in the smart home, are providing a persistent 'live' link to human activity in the private sphere it represents a qualitative shift in data sourcing and capture. Surveillance and monitoring technologies like DRM and embedded home systems of the kind previewed in the Microsoft Home and MIT's House_n are uniquely positioned to observe private life. They are incorporated into the personal and private physical environment of the domestic sphere itself. Monitoring technologies designed for the home are *written* right into the physical

structure in the case of ambient 'intelligent' systems; quite literally they are placed *into* the material space of private life. The same can be said of DRM systems running on personal digital devices. They persistently capture data in a wholly new and intimate environment not previously visible to the state or the market. It is quite remarkable that these systems have been developed and deployed with little effective resistance.[35]

These transformations are part of a broad re-mapping of private space from which personal data is collected and routed out to the market sphere. In particular, it makes the collection of personality-based data appear routine and places the home in the service of the market. Privacy of place cannot exist in/of the flows of the network. It is replaced by informational privacy in which the subject is reduced to data object and encoded. The smart home has become a communications node; half a space of flows and the other of place.

As private space is altered by code so too is individual privacy as the tactics and activities of the individual in private life are increasingly exposed by the very systems intended to make domestic space and living 'smart' and privatized. Where once the home could only be transgressed by some physical or material presence such as a visitor or intruder, the home has become permeated throughout the twentieth century by utilities delivery systems, telephones, television and radio and increasingly sophisticated ICTs (Shapiro 1998, 276). The codes (software) that monitor the homebody nudge the home

35 It could be argued that the Sony-BMG fiasco involving DRM-based root-kits installed automatically by the affected music CD spawned considerable resistance through a class action lawsuit (settled with Sony) (eff.org 2006). Solutions that are developed to break copy protection encryption are also a form of resistance (see doubleTwist.com).

space ever closer to the space of flows taking with it a flood of personally-identifiable and personality-based data.

In Chapter One I invoked Mitchell's notion of the logic prison. I view logic prisons as an apt metaphor for codes of control that structure and contain places and spaces. Pervasive systems and sophisticated ICTs in/of the home are designed to make living easy through customization and seamlessly connected systems of control. TPMs and DRMs allow or block access to digital media trading convenient delivery and reception for constant monitoring of private life. These systems are predicated on zones of inclusion and exclusion and access and denial of access binaries that operate as codes of control effectively turning the smart home into a personalized logic prison. This logic prison efficiently collects, authenticates and encodes personality-based data for ready transport to the flows of the network society. It is a logic prison, I suggest, that aids the collection and dispersal of personality-based data which ultimately contribute a subtly different kind of personal information to the flows, seeding the promulgation of the doppelganger effect.

Chapter Three

Traces and Databases: Identity redux

> Reproduction is diabolical in its very essence; it makes something fundamental vacillate.[36]

As personal data from all the collection points so far discussed circulate in the flows, it assumes great potentiality. Any single fact or cluster of facts can be pulled together to reconstitute an individual's identity in cyberspace in limitless ways. In this chapter, I will focus my analysis on virtual doubles or digital versions as traces of the natural person reproduced from facts collected about them reassembled in/by databases. I will set up the framework for digital personae by briefly reviewing the processes involved in the data cycle of collection, analysis, and dispersal and set out how facts about individuals become encoded as objects of analysis.

I have chosen a triptych of sorts around which to discuss metaphors of control in relation to personal information. First, I will explore the model put forward by some legal scholars concerned primarily with protecting informational privacy in an electronic persona as a 'propertized' version of ourselves — "a compilation of bits of personal information concerning the individual" (Mell 1996, 34-35).[37] There are several perspectives in the debate to protect informational privacy in this way and most centre around some form or container to control access to personal information and manage online identity and reputation. As it stands today, data analyzers claim a property right in,

---

36 Baudrillard (1988, 182, n.1).

37 The electronic persona can be distinguished in my work from an avatar or graphic representation an individual chooses or is assigned in cyberspace or a virtual environment. Examples of an avatar would be the graphic icon an individual selects as their representation in instant messaging applications, on social networking sites, or in video games.

and control over, the analysis and information produced from collected personal data.

Secondly, I will analyze the notion of the data double referenced in surveillance studies which is not a propertized persona imbued with privately owned personal facts but a more transient virtual figure drawn together from any number of personal data sources in the flows out of a "surveillant assemblage" (Haggerty and Ericson 2000). Here too control is projected by the data analyzers over the data and information they produce.

Finally, I will discuss the digital doppelganger as the reproduction of all possible renderings, permutations, and reproductions of the individual, good and bad, old and new. Control is evident in the protocols that organize the flows, but as I will demonstrate, this model persona abandons any notion of control over personal facts by either the individual or the data analyzers to the logic of the database management system (DBMS). The digital doppelganger encompasses the multiple and imitable ways the natural person can be reconstituted in cyberspace. I suggest that there is no formula for placing control in the 'hands' of the natural person or any formulation of a protected virtual persona that could govern what happens to data after it enters the flows of the network society.

Capture and encoding

In this contemporary moment, governments are decentralized, even becoming distributed relying on ever more strategies of citizen self-management to govern at a distance. Mark Poster advises that modern states would not exist in their present form without databases which have a stabilizing effect by producing "knowledge of the population available to coercive institutions at every level" (1996, 189). In the previous chapter I outlined the ways in which surveillance technologies and techniques in/of the

smart home collect personal data and route it out to the flows, but what transpires in the data cycle after collection?

Prior to the creation of virtual identity(ies) personal data must be collected, processed, analyzed, sorted and otherwise manipulated by an organization with specific interests and capabilities in data analysis. Any type of organization can collect data. Private and public sector organizations engage in "dataveillance" as do not-for-profit and civil society groups. In Chapter Two modes of data collection in/of the home were catalogued. There are, however, also many other points of capture that submit data to the flows mixing with personality-based data from the home.

Data collection occurs in contexts such as: online and off-line point-of-sale (POS) transactions; web surfing and browser cookie deposit; email and instant messaging; revenue and taxation; health system access; file downloads and uploads; print and online media subscriptions; insurance and financial transactions; surveillance cameras; digital TV systems; cell phones and wireline phones; iPods and Blackberries; loyalty card programs; utilities accounts and usage; and computer and device software upgrades, to name but a few (Lyon 2001, 2003; Elmer 2004, 53-71). Personal data can include discrete facts such as: name, biometrics, passwords, aliases/nicknames, employment, DNA, age, geographical location, mail address, email address, and cross-referenced date and time data (Marx 2006, 79).

While any company can engage in data collection, the functional analysis of the data post-collection is undertaken by specialized corporate data analyzers through data mining. Data mining is classically defined as "knowledge discovery in databases"

directed at finding patterns in the data that ultimately guide decision-making, inferencing and forecasting (Turban and Aronson 2001, 145). Natural language words, phrases, and descriptive characteristics such as personal facts are collected, encoded and recorded in pre-defined databases (Feelders, Daniels, Holsheimer 2000). This capture and encoding of personal facts as raw (unprocessed) data produces coded objects that are readable by databases. Data mining employs sophisticated algorithms to sort and aggregate data, sifting and searching for patterns that mark out behaviours, preferences, motivation, spending and consumption patterns among profiled groups of consumers as well as individuals in the market (Turban and Aronson 2001, 146; see also Gandy 2006; Elmer 2004).

Data analyzers use sophisticated digital technologies as a tool to capture data and turn it into information and ultimately knowledge. This suggests a hierarchy of attributes and value. Each new arc from data to information to knowledge expands the value of the output. From the binary ones and zeros of every action and transaction come the bits that coalesce into data that combine into analytical categories that become information from which knowledge is produced. Data analyzers use the raw material of data to produce high value information and knowledge (Gandy 2006, 364-369; see also Feelders, Daniels, Holsheimer 2000). For corporations specialized in data analysis, knowledge output is a corporate asset and revenue source; their business model centres around providing data analysis services and knowledge production.

It is the action of amassing the data combined with the analysis functions and finally the output that data analyzers use to construct a Lockean argument for a property right in

the information as product (Litman 2000, 1300; see also Lipton 2004). Data analyzers argue that data, as a raw material, is meaningless on its own and only after they mix their labour (analysis) with the raw data is something of value produced as a marketable commodity over which they have proprietary interest (Lipton 2004). From a purely Lockean market perspective this may be so.

Curiously though, for the individual caught up in the data cycle of collection, analysis, and dispersal what begins as a complex and nuanced collection of personal information gathered in an original transaction is demoted at the point of contact with the database system to a collection of facts rendered as data objects. As the data passes through the analysis phase it is re-factored from data object to a cluster of meaningful facts in a profile and re-written once again as information. The change is not insignificant. What emerges post-analysis is entirely abstracted from the context of information surrounding the natural person in the material world.[38] Thus, at the point of collection the individual gives up any control over how they will later be analyzed, profiled and interpreted by corporate and government information consumers.

Once data is captured and encoded in a database it is available for profiling. Profiling is an "attempt to account for the unknown" and ultimately to govern individuals by tracking patterns of behaviour (Elmer 2004, 134). It is predictive: it uses "data gathered in the past in order to generate descriptions about events that *may occur in the future*" (Gandy 2006, 370-371; emphasis mine).

Buttressing this activity is what Elmer refers to as the oscillation between reward

38 The notion of context is presented in Helen Nissenbaum's notion of privacy and "contextual integrity" wherein she links privacy protection to norms of specific context.

and punishment between the consumer and provider of goods and services. At the start of the data cycle, the corporate provider makes "subtle requests and not so subtle commands for personal information" in which refusal to provide personal details results in a blunt refusal of goods and services (Elmer 2004, 6). Surveillance, in Elmer's view, does not account for the "multiplicity of processes" that request data as a requirement for access to new information technologies whether in the home or beyond (2004, 5).

Elmer's perspective echoes earlier work in this area. Lyon (1994) has also examined the series of solicitations and seductions in which the individual participates willingly in their own surveillance by trading access to personal information for access to goods and services. Gandy has observed that "the panoptic sort increases the ability of organized interests... to identify, isolate, and communicate differentially with individuals ... [and] increase the precision with which individuals are classified according to their perceived value in the marketplace" (1993, 2). Each of these scholars reflects what Poster and Zwick and Dholakia refer to as the interpellation of the individual into a willing subject of surveillance. Individuals as consumers of products and services "participate in the formation and population of their own data records by committing simple consumption acts" (Zwick and Dholakia 2004, 22; see also Poster 1996).

What is evident is that surveillance is much more than a simple act of monitoring but is part of a more complex dynamic which pits the individual consumer against the collective strength of corporations delving deeper and deeper into aspects of private life. The facts of individual life are captured and encoded and provide a "means of representing, sorting, collating, matching, profiling, regulating, [and] of generating

information" applicable to aspects of governmentality and commerce (Dodge and Kitchin 2005b, 877). What model of control exercised by an individual over the use and application of their data could contain this apparatus and output of surveillance?

The electronic persona

Roger Clarke described the digital persona as a "model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual" (1994). Clarke's definition is a useful point of departure to explore the first form of the digital persona, the electronic persona. Proposals for a property right in personal information far exceed Clarke's original proposal in which he saw the digital persona as a passive creation comprised of data only.[39] The electronic persona, by comparison, is intended as a propertized container for personal information including aspects of personality furnished with rules governing its use under the direct control of an individual. Yet Clarke's definition captures two key elements that resonate within all three of the digital forms to be discussed in this chapter. He identifies the aspect of personality contained in collected data and its value as a 'stand-in' or proxy for the individual in data analysis and profiling (Clarke 1994).

In the previous chapter, I suggested that data collected in the home provides the flows with a new and rich source of personality-based facts about the individual in private life. A set of facts detailing personal habits, behaviours and routines that illuminate the choices and preferences individuals make in day to day living. Margaret

39 The electronic persona proposes an element of control exercised by the individual over their own personal information which is not part of Clarke's vision. Clarke also defines what he labels as "active digital personae" which are created as agents or 'bots' to carry out an automated activity in cyberspace (e.g. 'spider bots' or indexing services used by Google and Yahoo! search engines) but are not representations of an individual's personal facts (1994).

Radin (1982), in her classic essay on property and personhood, forcefully argues against property rights for aspects of personality. She resists the notion of the person in commodity form distinguishing between personal property rights and fungible property rights.[40] The former are inalienable rights that are essential to the person, to/of personality, and the latter are bound up in objects that can be traded without diminishing the individual's personhood (Radin 1982). Radin also makes an important association, I think, between personhood and personality in that "The more closely connected with personhood, the stronger the entitlement" or claim to personal property rights that are not fungible (1982, 986). Thus, aspects of personality collected by surveillance systems in the home that reveal intimate life choices, it can be argued, demean the person.

The proposal to protect personal facts as objects of property teeters on the edge of intellectual property, suggesting some sort of right to reproduce or copy personal facts in commercial transactions would need to be established (Lessig 2003). Margaret Davies and Ngaire Naffine stress that "objects of intellectual property are abstract rather than physical" and are thus separable without diminishing the natural person (2001, 125-129). This perspective shifts aspects of personality and personal facts about the individual toward the commodity form consumed in/by the market for data; personal facts easily become objects of commerce under this model.

The electronic persona as a legal construct finds its way into the debate around informational privacy and data protection as a means to empower the individual to have

---

40 The collection of rights expressed in personality rights are "privacy, image, voice, bodily integrity, name, and reputation" and clearly some of these, such as image, are considered fungible in some jurisdictions (Reiter 2002, 680). The right of publicity in the USA (though it varies by state) protects the image as public persona which is fully fungible as a species of intellectual property (ibid.).

control over their personal information (Mell 1996; Cohen 2000). While data protection policies may dictate how and for what stated purpose organizations can collect personal data, such policies do not offer any mechanism for the individual to exercise real control over how the data is reassembled by databases. The individual does not control how they are profiled, how their identity is reconstituted, nor control the conclusions drawn from the analysis. Data protection and informational privacy laws do not enable the individual to recall personal facts from circulation nor extend meaningful control over the analytical purpose of the file over time and by third parties.[41] The electronic persona is proposed as an instrument of control over these functions.

Patricia Mell (1996) makes a strong argument for the propertized persona in cyberspace.[42] In her definition, the electronic persona would be inscribed with preferences, facts, and permissions to enable the individual of the material world, the natural person, to control disclosure, use, representation and rules for the sale of their personal data in the virtual sphere (Mell, 1996). By this definition, the electronic persona would also enable online identity and reputation management to offset the misuse and potential misrepresentation of individual identity in cyberspace.[43]

Mell's proposal borrows from elements of copyright, American-style publicity rights and right of privacy. An electronic persona that fuses right of publicity and right of

---

41 It can be argued that data protection and informational privacy legislation and self-governing FIPs offer this protection by describing data policies to which an individual consents in an offer or transaction for services or goods. However, I am arguing that meaningful control is not possible over the manner and method of reproducing identity out of the collection of facts. This will be explored in more detail in Chapter Five.

42 Mell's (1996) essay does not use the term 'cyberspace' coined by author William Gibson and popularized in *Neuromancer* (1984); rather she refers to virtual space as the "electronic wilderness" but I will use 'cyberspace' in its place to maintain consistency throughout the thesis.

43 As it stands now, online reputation and identity management consist of a jumble of market solutions. ReputationDefender promises to "Find out everything that's being said about you online and get rid of the content you don't like. Let us make sure that your reputation is not hurt by information posted online." (reputationdefender.com).

privacy is merging seemingly opposable forces by her definition (Mell 1996, 35). The right of privacy signifies a right to individual solitude or non-disclosure of information while the right of publicity assumes individual exposure (Mell 1996, 35; see also Nimmer 1954).[44] Mell's electronic persona tilts toward right of publicity to govern exposure and control over the persona folding personal information into a copyright-like scheme for protection of personal facts and then attaching fair information principles to this bundle of rights to govern collection, use, and disclosure (1996, 6, 35-36). This model would require a new form of intellectual property that attaches the above elements to an electronic persona controlled by the natural person.

Applying the American right of publicity as an overall reference model for this electronic persona has some attractions. A fuller discussion of the right of publicity is beyond my thesis, but some aspects of this model are useful to the electronic persona. In its classic definition, the right of publicity protects the commercial value of an individual's identity or persona (Nimmer 1954; Mell 1996). In many jurisdictions this protection is descendible and thus the publicity persona 'lives on' after death of the natural person as part of the estate (Wall 2003).[45] A key feature of the publicity persona is its ability to appear simultaneously across the space-time continuum; meaning, it can

---

44 Colin H.H. McNairn and Alexander K. Scott (2001, Chapter 3) articulate the confusing history in Canadian courts over whether to recognize a common law tort of invasion of privacy. Some Canadian provinces have recognized a tort of invasion of privacy and Quebec's civil law states that privacy is an essential value to be protected and merits action when violated (47-50). In Canada, there is no right of publicity in which are defined a set of rights and obligations for the exploitation of one's own persona for commercial gain. Under Canadian law, individuals can claim for the misappropriation of personality when someone uses their likeness for commercial gain without permission (McNairn and Scott 2001). They cannot, however, find protection in a right of publicity as a species of intellectual property (ibid.; Howell, 1998).

45 In many jurisdictions in the USA, it is good to be dead. Celebrities and public figures can engage publicity rights management firms to commercialize their image for profit during life and to benefit their estate after death. Publicity rights management company CMG Worldwide (http://www.cmgworldwide.com/) whose slogan should be the Monty Pythonesque, "Bring out yer dead!," aggressively manage and defend the rights of their clients, the living and the dead. On February 25, 2007 they were "welcoming" the late Marlon Brando as a client.

be in material space and virtual space at the same time licensed to multiple users even after death of the public figure. The electronic persona also has simultaneity and can exist in perpetuity — the archival process of cyberspace ensuring it may well outlive the natural person. In theory, the electronic persona would be technologically enabled but personally defined and imprinted with individual preference moving through cyberspace as if time did not matter.[46]

However, where the publicity persona is managed through licensing in the material world which governs its representation regardless of format (virtual or real, radio, Internet, print, and/or TV) the electronic persona can split in a million ways conjuring up identities that cannot guarantee the accurate representation of the natural person in cyberspace. The publicity model is based on the notion of a central, propertized and governable *original* over which the assignee exercises control in the reproduction and representation of the image. For the electronic persona there is no such original.[47] Profiling and analysis draw from a set of facts about the natural person to reconstitute but one *version* of identity; change the bits in the compilation and a different version, or copy, of identity emerges. Such weaknesses abound in the electronic persona.

Mell is by no means alone in exploring control models for personal information. Julie Cohen proposes a "dynamic theory of informational privacy" in which technology-enabled privacy principles embed preferences and permissions in collected data objects on behalf of the natural person (2000, 1437) which could then presumably reside in

---

46 Would ownership of the electronic persona be descendible? Why and how managing the electronic persona of a dead person would be of value to the living is not immediately obvious to me, however, there may be residual value to data analyzers in incorporating historical data in other analytic scenarios.

47 Poster invokes Baudrillard's notion of the simulacrum by using the example of a music recording comprised of separate tracks and mixed, recorded and then copied; there is no original (2001, 10).

virtual space within a "tagged" persona. The onus remains with the individual to manually input what would inevitably be an overwhelming array of choices, permissions and allowances in a continual exercise to manage these indicia over time. Ultimately, Cohen retreats from this property model in favour of legislated privacy options. There is active research, however, into the model she discusses. "Obligation specification language" can be attached to a file to embed privacy preferences which describe the terms and conditions governing the owner and the user of the information (Hilty *et al.* 2007, 538). I argue that file augmentation of this sort is not constraining the circulation of personal data in the flows simply appending a rule to it. The information about the individual is still out there; the multiples of cyberspace persist.

The electronic persona, then, is centred around providing a modicum of control directed through one defined and singular individual in the material world. It does not, however, constrain the actual collection and circulation of personal facts nor the repeatable and imitable ways the individual is reproduced in cyberspace. Can this proposal offer any means to control how the individual is represented in cyberspace? How does it offer control over which elements and facts of the natural person are selected from the flows to manufacture identities for profiling?

Much has been written on the social construction of the self and the distinction between the person and role as dependent on social definition. Erving Goffman wrote extensively on the performative aspects of the self "behind a role" and the "presentation of the self" in the material world (Goffman 1997). Goffman's work suggests to me that in the contemporary network society the individual is also invested in preserving a

particular *version* of the self and controlling that representation in cyberspace.[48] My analysis demonstrates that an electronic persona cannot extend meaningful management and control over representation of the self into cyberspace. The performative aspect of identity 'versioning' in cyberspace resides within databases which organize subjects into objects, writing out identity to match specific analytical parameters (Poster 1996,189).

Poster draws upon Foucault's concept of discourse and applies it to databases "because they effect a constitution of the subject" thus objectifying and producing individuals with dislocated, dispersed identities within cyberspace (1996, 182, 190). The individual is "interpellated by the superpanopticon" (Poster 1996, 184) or surveillance architecture into providing data requested by public and private organizations. This theory dislodges the notion of the centred, liberal self with its "'subjectified' interiority" upon which certain rights and freedoms attach (Poster 1996, 190). The liberal subject is said to have agency over its self and a self-determining purpose exercised through choice. In the context of my thesis and a later discussion on informational privacy, the liberal subject is said to choose when to be private and when to disclose information; however, it is this very act of agency that is challenged by the discursive power of the database.

The productive power of the database, in Poster's conception, routinely disturbs the coherent and rational subject of liberal ideology the electronic persona seeks to stabilize in cyberspace. The database is to Poster both a "performative machine" and a "perfect writing machine" inscribing new identities upon the subject (1996, 186, 184). The

---

48 I am thinking here of the ways individuals customize or personalize their online avatars to look a certain way within an online social networking environment or other virtual world. An individual can describe themselves any way they like using any number of terms and attributes that may or may not be factual or indeed be anything like the natural person.

operational aspects of databases bridge the ethereal and the technical to reveal the possibility that forces are at work that cannot be brought under control by the natural person. Once launched the database technologies that collect, move, and shape raw personal data into information hold the potential to recreate the individual in unexpected and unanticipated ways. This exposes an aspect of the doppelganger effect to which I will return in the next chapter.

The establishment of a property right in the electronic persona and all its many virtual instantiations exposes the difficulty of trying to protect the natural person in one defined category among many possibilities in cyberspace. The identity reconstituted by a data analyzer from the personal data stored in the electronic persona is but an object of analysis; the data processor 'sees' a collection of data from which they can produce the subject as a "known and knowable object" (Zwick and Dholakia 2004, 4). Here the discursive power of the database is at work. The individual's identity is virtually *re-written* by a database system whose language is complex and object-oriented.

Even if the individual exerts an ownership over their personal facts they do not own or control the manner, method, and outcome of information produced through data mining and profiling. Each digitized instance of the persona reconstitutes an identity fractured from the self the natural person seeks to represent, and control representation of, in both the material and virtual worlds.

The data double

The theme of a virtual double or digital persona are common in analyses and commentary addressing surveillance in society. Work in this area often takes as a common starting point George Orwell's novel, *1984*, in which Big Brother spies on the population with panoptic totality. The proliferation and expansion of surveillance systems would likely exceed Orwell's wildest nightmare; however, he did configure the notion of persistent data collection (even at home) with surprising clarity. Research into monitoring practices, however, offers a more critical reflection on systems of surveillance and the vast repositories of data collected and retained by state and private organizations far beyond Orwellian predictions.

In Chapter One, I reviewed Haggerty and Ericson's concept of the surveillant assemblage as an extension of Deleuze and Guattari's notion of assemblages that are comprised of multiple entities and phenomena in flows. Assemblages can collate any object in/of the flows including people, materials, knowledge and institutions. The assemblage is transitory and brief. It represents the convergence of flows into a moment of analysis; the assemblage freezes the flow temporarily and spatially for analytic purposes and then breaks apart (Haggerty and Ericson 2000, 608-609). What makes the surveillant assemblage so powerful is its potentiality and its instability (Haggerty and Ericson 2000); it forms, separates and re-forms in a fluid response to requests for information by data analyzers.

Haggerty and Ericson argue that captured flows coalesce into systems of domination characterized as "desires for control, governance, security, profit and entertainment"

(2000, 609). Observation and surveillance are hierarchical; the targeting of the objects/subjects varies across socioeconomic class, race, ethnicity, age, and gender lines.[49] This is in keeping with the operative characteristics of neoliberal governmentality whereby surveillance enables observation of targeted populations but extends to marketing and law enforcement projects as well. The surveillant assemblage is also productive and "operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows" (Haggerty and Ericson 2000, 606). It is from this dynamic assemblage of flows, entities, captured phenomena, and objects of analysis that the data double emerges.

The data double is the second form in the triptych of digital personae and diverges sharply from the self-governable object of relations represented in the electronic persona. The reconstitution of the data double from the surveillant assemblage represents the "formation and coalescence of a new type of body, a form of becoming which transcends human corporeality and reduces flesh to pure information" (Haggerty and Ericson 2000, 613). "Pure information" is not so much extracted from a well of facts as it is written out of a moment of analysis by the analytic engine of the database. Where the electronic persona is theorized as an instrument of authorial proprietorship over personal data and subsequent identities in which profits would be split between the natural person exercising the persona and the data analyzers' claim over the information, the data double is but a catalyst. It burns up in the analytic calculus from data to productive information.

---

49 Haggerty and Ericson point out that the poor make regular contact with surveillance systems through social assistance and criminal justice encounters, whereas the middle class through more routine documentation and monitoring (2000, 118). Middle class surveillance is often 'self-inflicted' based on consumption – this is evident in the pervasive systems of the smart home that require involvement by individuals or tacit acceptance as in DRM systems.

Data is briefly extracted and compiled to satisfy a request for information by the data analyzer and the data double fleetingly gains form as an object of analysis and then decomposes. It has simultaneity; there can be many thousands regenerating at once in the swirl of flows, but each is finite. It lives the brief life of a fruit fly and just as quickly it dies. Its very instability shatters any suggestion of control the natural person in the material world may attempt to assert over its form and function. This model, I argue, more closely approximates the dynamism and magnitude of force in the flows of the network society.

The notion of the data double surely references an individual but Haggerty and Ericson (2000, 614) suggest it transcends real representation and does not explicitly incorporate identity in its fleeting incarnation. The "discrete flows" that contain facts and indicia which merge in a profile about the individual are absent meaningful identity in their rendering. On this point I disagree; the facts and details about the individual contained in and reassembled by databases have real-world implications and are intended to 'look like' the natural person for the purposes of analysis and decision-making. The productive force unleashed by the database has a consequential outcome for the natural person and thus feels quite 'real.'

The data double captures the element of velocity in/of the flows in which the collection-analysis-dispersal data cycle operates. I argue that identity is reconstituted in rapid machinic flashes and imprinted in a receiving system for analytical purposes and then discarded. In this instance, the reconstruction of identity and the management and control of identity are far beyond the purview of the individual but what is generated by

the database is at the very least informational identity. This effectively challenges any notion of control over the reproduction of identity and profile by the data analyzers.

Data analyzers, or indeed a range of companies that collect, analyze and sell such information services, project a powerful Lockean model of control. Control appears to be exercised by the data analyzer through their claim of ownership of the data and the output (information).[50] Here the emphasis is shifted from the electronic persona as the locus of/for control to the technologies of data collection and the data analyzers as the *emulation* of control.

Digital doppelgangers

I chose the preceding models of digital personae because each can map to a particular philosophy about control. Formal legal proposals tend toward solutions offering control over the electronic persona and personal facts ascribed to it as property or in legal protection conferred by forms and rules aligned with intellectual property law. The data double abandons all notions of control in the fleeting object of analysis itself and points to control by the data analyzers who capture and profile data from the surveillant assemblage.

I propose the digital doppelganger as a more apt metaphor for the network society. Here the emphasis is shifted from the subject represented by the electronic persona as the locus of/for control and from the technologies of data collection and analysis to the

50 Companies operating in the data market are not always clear about what happens to data they receive to fulfill a data processing contract that results in information – it could be retained and/or resold. Data analysis is a for fee service and the output, the information in the form of predictive analysis, consumer profiles, and marketing intelligence is highly valued. Some companies collect data or buy data which is then processed and offered for sale to targeted companies in a particular market segment (CIPPIC 2006). Canadian companies working in this space include: Boire Filler Group; Cornerstone; and Resolve Corporation.

database itself as control. The individual does not control nor understand the language of the database executing the rules and techniques of analysis and profiling (Poster 1996; see also Zwick and Dholakia 2004, 5, 7).

The digital doppelganger is a new mode of subjectivity: it represents the subject as object reassembled in/by the database. This new mode of subjectivity has its own form and effect. Digital doppelgangers are the form that appear in the network society out of the flows as the multiples of cyberspace and the effect, or consequential outcome, is in its ability to make things of consequence happen for the natural person. The doppelganger effect occurs precisely because the rhizomatic undergrowth comprising the distributed pathways of the network society carry bits of personal data that spread and proliferate with a certain amount of unpredictability.

The performative aspect of the database, with its productive power to inscribe new identities on the subject (Poster 1996), gives substance to the doppelganger effect producing consequential outcomes, good and bad, for the natural person. Control can be emulated by those who own the means of information production (the data analyzers), but ultimately control resides within the "perfect writing machine" as it reproduces the multiples of cyberspace from collected personal facts and indicia.

William Bogard, in his re-working of Deleuze's societies of control thesis suggests that "control is now an inclusive, continuous, and virtual function, traversing every level ... simultaneously molecular and planetary, no longer limited by walls or schedules." (Bogard 2006a, 59). It suggests that control is nowhere in particular, certainly not in the object of analysis whether an electronic persona or data double, but everywhere dispersed

and disarticulated echoing Poster's superpanopticon. In Bogard's vision, the self is "endlessly divisible" (2006a, 72) and therefore each reconstitution of personal facts into a digital doppelganger creates a new identity cobbled together by pieces of data and devoid of context.

The doppelganger has historically been an object of Romantic-era fiction and hence much of the scholarship examining its place in western folklore and history is translated through the optic of critical literary studies. Literary analysis has in turn swept up various theoretical frameworks to explicate the double motif including psychoanalysis incorporating Sigmund Freud's notion of the "uncanny," Marxist analysis and postmodern perspectives on multiplicity and identity.[51] It is not my intention to take up postmodern literature analysis itself, but rather draw on the techniques and understanding evident in the critical nature of such studies in which motifs of representation and subjectivity are challenged.

Milica Živković suggests that the double resists and opposes the established order of society because of its potentiality; the possibility of "innumerable other selves" that dilute the dominant system where it is reproduced in the individual (2000, 7). The digital doppelganger amplifies this disruptive force. It defies coherency. The multiple identities of cyberspace, in whatever form, diminish the natural person. The concept of the coherent, rational liberal self is destabilized by doubling, or multiplying identities, representation and misrepresentation. The Enlightenment values embedded in liberalism

51 Unpacking Freud's notion of the "uncanny" far exceeds the objectives of my thesis and a complete analysis is therefore not possible. However, the "uncanny" is Freud's explanation for the occurrence of the unfamiliar within something that should be familiar such as being startled by one's own appearance in a mirror (it should look familiar and yet does not). In relation to the doppelganger or double, the "uncanny" suggests that what should appear identical does not; that the double signals repressed memory and thought accompanied by a feeling of dread (Freud 1919).

that coalesced around a singular, rational, autonomous self are now threatened by opposing forces of irrationality and multiple selves in cyberspace (Bartlett 2005, 39).

In Romantic-era fiction the doppelganger always has some kind of flaw that renders this double at cross-purposes to the natural person. The doppelganger is always at a distance from the human and the "replication is always unbalanced ... at least one significant trait nullified ... [and] seeming congruences frayed" (Alexander 1998, 16). In cyberspace the digital doppelganger suffers from a similar disconnection or incongruent effect. Databases reproduce identity from a selection of facts abstracted from contextual meaning out of which identity is redrawn in a manner and by a method relevant only to the data analyzer. The resulting profile does not accurately represent the individual, but displays a set of facts clustered as information for the purposes of decision-making directed at a particular outcome.

I was recently profiled for an insurance claim. My claim was returned to me with a pitiful contribution toward my overall cost with the note that my age, hearing loss, income and geographical location suggested the cost of my hearing instruments (hearing aids) should not have exceeded an established amount projected for my profile. Though I submitted background information, medical history and test results it is evident those were not selected as part of the analysis for my claim. However, for the purposes of insurance profiling this claim history will be embedded in the database. The onus is now on me to prove that I lost my hearing as teenager as a result of a genetic disorder rather than be categorized as an individual within a profiled group of middle-aged hard-of-hearing people mapped to a particular outcome that does not reflect my unique

requirements. My digital doppelganger apparently hears much better than I do.

It is, though, the effect of this "uninvited intruder" (Bartlett 2005) or digital doppelganger on my life choices and options that most frustrates attempts at controlling how I am profiled in the above example. By consenting to access of my records by the insurance provider I did not get to influence *how* I was profiled. My identity was reproduced by the database absent any contextual input from me.

Reproductions of the self in cyberspace born out of the flows can be benign and resolve out of 'legitimate' queries by data analyzers, but they can also sweep up so-called bad data that is out of date, unverified, and factually incorrect, or simply ignore certain facts about the natural person. The data that circulates in the flows creates what Dodge and Kitchin label as the "capta shadow" (2005b, 858).[52] The capta shadow contains everything from discrete facts about the individual residing in unique databases such as for insurance or health purposes as well as the identity codes of passports and drivers licenses which in turn connect and relate to a set of data about the individual (Dodge and Kitchin 2005b). The capta shadow is continuously growing, moving in parallel with the individual. It is the digital doppelganger, I suggest, that fixes the capta shadow in a moment of analytical creation "making explicit what is implicit, present what is latent" (Alexander 1998, 39).

The digital doppelganger is an "inveterate performer of identity" (Webber 1996, 3) enacted by databases and thus mediated by technology.[53] Because the capta shadow has

---

52 *Capta* are single units of data extracted from a wider set of data (Dodge and Kitchin 2005b, 858). The *capta shadow* encompasses all the bits of data about an individual in the flows.

53 Webber (1996, 3) views the doppelganger or double as the "performative character of the subject" engaged in a process of "enactments of identity always mediated by the other self. "

grown so large, the digital doppelganger's constant presence precedes the natural person (Stalder 2002). The individual checks in at the airline counter and the customs desk and numerous digital doppelgangers become visible and non-negotiable already fixed in the security database. The rule-bound codes of control, the organizing properties in databases that root the digital doppelganger in silicon, give it substance and staying power. The individual does not have control over its inception, its form, content or the extent of information contained by it (Dodge and Kitchin 2005 b, 859). Dodge and Kitchin suggest that it is the capta shadow that makes the human form machine readable – the collection of facts about the natural person assembled into a pattern understood by databases and the DBMS. The digital doppelganger thus plugs into the logic of the "machinic complex" in which multiple databases are configured to converge into massive data applications.[54]

Conclusion

Digital doppelgangers are concurrent with other doppelgangers and have persistence in and of the flows. This form can be created anew out of a moment of analysis or retrieved from an archived profile post-analysis. It does not dissolve or self-destruct. It is left undeleted. The torrent of flows in the network society render the individual as an indistinguishable form except where rule-bound, logical systems select and analyze the individual as an object of analysis.

The digital doppelganger is the individual rewritten over and over by databases which are in turn re-catalogued, archived, cross-referenced, and re-incorporated into

54 The term "machinic complex" is borrowed from John Urry's (2000, 60) descriptive term for "humans and machines combined in new and intricate 'machinic complexes'." Urry applies this term specifically in the context of his examination of new mobilities or "monsters of automobility" in the context of cars and humans but it fits equally well to the notion of humans and software-driven technology.

meta-data stored in new databases. A cyclical routine of inscription upon inscription generating its own mode of subjectivity. These new identities reduce the complex natural person to multiple data objects within an intelligent system capable of sophisticated analysis and information production. This suggests the modern liberal subject is not the self-determining and purposeful agent of classic liberal philosophy.

The doppelganger effect, as the next chapter will illustrate, is a constant and reproducing effect that is part of the network society. It is not something to be controlled by material regulation or formal legal rules but is to be considered in an ongoing effort to understand what possible effects continue in the ever-increasing collection and dispersal of personal data.

Chapter Four

The Consequential Outcomes of Perfect Writing Machines

> Population Census have got him down as dormant, the Central Collective Storehouse computer has got him down as deleted, and the Information Retrieval have got him down as inoperative... Security has him down as excised, [and] Admin have him down as completed.[54]

In the dystopian society envisioned by director Terry Gilliam in the movie, *Brazil* (1985), a totalitarian state collects information about its citizens with bureaucratic (in)efficiency and subjects them to complicated information systems of Orwellian proportions. Mistakes in the information system can result in unintended consequences for citizens and require costly and complex encounters with the Ministry of Information to disentangle matters of identity confusion. While Gilliam takes mistaken identity to far extremes, the above quotation illustrates the multiple ways identity is reproduced by attributes about the natural person absent any material context. The identities of the individual created by the database as the "perfect writing machine" may be wrong or right, timely or historically inaccurate, but regardless, the output is of some consequence to the natural person. The multiple ways identity is written out of the database is entirely beyond the control of the natural person. This is central to the doppelganger effect.

The individual is complicit in the collection of data and subsequent reproduction of their identity in cyberspace whether intentionally through daily transactions in the wider world or unintentionally by engaging with systems that monitor the "little tactics of the habitat." The doppelganger effect is in every single invocation of identity in the virtual

---

54 The character Mr Kurtzman, a mid-level bureaucrat in the Ministry of Information, in director Terry Gilliam's dystopian film, *Brazil* (1985).

world – it is in every moment of contact between the natural person and points of capture as they contribute to databases through their consumptive practices. Borrowing ever so slightly from chaos theory which informs how distributed systems (and pervasive systems) function, the multiples of cyberspace created by the "perfect writing machine" or database operate successfully within an inherently chaotic system when organized by codes of control. Codes of control, whether as the database management system (DBMS) or network protocols, are the coordinating principle which organize all kinds of information in a rational, logical and seemingly accurate fashion in the information flows of the network society.

My aim in this chapter is to link the postmodernist claim of multiplicity in/of identity in cyberspace with the productive power of databases to inscribe new identities upon the subject (Poster 1996; Zwick and Dholakia 2004). The doppelganger effect is triggered by this crucial mechanism in which "perfect writing machines" create consequential outcomes for the natural person.

I will begin this chapter with a discussion of the doppelganger effect and the multi-threaded inputs that aid its creation. It gives rise to instances of identity confusion or unintended consequences for the natural person in the material world as often as reproducing intended abstractions such as marketing profiles claiming to represent the individual. The effect is a perfect storm of identity details, databases and codes of control and protocols dispersed along the distributed network.

In this chapter, I will examine how the doppelganger effect manifests in ways relevant to the natural person. While I propose the effect is real and constant even when

unseen or unexperienced, it is most apparent through data breaches and exposures and in unintended consequences that play out for the individual in both material and virtual space. This is not to suggest that the doppelganger effect is only a negative consequence; it is not, but it is felt more acutely when its effect has a negative outcome.

I will address four different examples that expose the doppelganger effect. In the first two examples I will discuss how the consolidation of personal records and databases contribute to identity fraud which is particularly significant for the doppelganger effect. The first example is the theft of customer records from a private sector company, the TJX Corporation and second, the loss of citizen records by Her Majesty's Revenue and Customs Service in the UK (HMRC). The final two examples illustrate specific instances of identity confusion and reputation. The third example relates to the sexual assault case involving an American basketball player, Kobe Bryant and finally, the last to a less devastating example involving discrepancies in a credit report.

The Doppelganger Effect

The doppelganger effect is not simply born at the moment the subject is rendered as object or the moment profiling begins. It begins at different moments, in many different spaces, through complex, contingent happenings within the flows. Its genesis is in the subtle re-territorialization of spaces in the network society that fold more and more space of places into the space of flows. Its beginnings are found in the evolving sources and types of identifying characteristics captured as personality-based data. It is conjured by the persistent reproduction of identity multiples, the digital doppelgangers, out of the facts and minutiae of the flows. The doppelganger effect encompasses every profile,

avatar, digital persona, personal identification code, and account name. It represents every rational calculus and actuarial output alongside every misrepresentation, miscalculation, and mistaken identity.

The doppelganger effect is the result of a constellation of effects: the productive/discursive power of the database; collected personal data; codes of control and protocols; and distributed networking. This peculiar constellation of phenomena are continuously productive and generative. Not every aspect need be operative to engage the doppelganger effect. The distributed network is in continuous modulation, forming, breaking and re-forming rhizomatic linkages efficiently brokered by network protocols and codes of control enabling data to move in the flows. Personal data is in constant generation through acts of consumption, reception and production as are the databases to sort, catalogue and profile the captured data. Other contingencies enable this constellation of effects to emerge: the space of place transmuting to the place of flows; the dominance of informational privacy; the flows of the network society; the Internet; and new technologies and sites of surveillance collecting and dispersing personality-based data.

Distributed chaos and control

The distributed model of both computing and networks is significant to the doppelganger effect as one of the constitutive elements that contributes to its emergence. Distributed computing is defined as "systems of relations between objects" where the focus is on the interconnectivity and flexibility of the "functional structure in the software" (Power 1990, 2). Pervasive systems rely on the distributed model to function and keep heterogeneous elements communicating. Historically, networks and computing

models emphasized the hardware aspects such as physical networking infrastructure including modems, cables, and processors, but contemporary computing is all about code or software (Power 1990, 2).

Distributed computing systems are designed to enable knowledge acquisition from distinct objects in the network and hence the database, discussed below, has co-evolved alongside the distributed model to collect and collate system information passed between network elements (Power 1990; 1993). This communication relies on rules or protocols to organize and coordinate data passed back and forth between entities on the network as well as out to the flows.

Alexander Galloway (2004), as referenced in Chapter One, takes up code and control in the network society, but does so by examining the protocols (code-based rules) that enable and organize network connections. Protocols can organize biological, informational, or any network by describing, enabling and enforcing rules to organize and coordinate data between entities in the network (Galloway 2004). While distributed networks are not themselves hierarchical, they can negotiate hierarchical relationships at the same time as they propagate through self-determining, autonomous programming that facilitates a distributed rhizomatic array of nodes and pathways (Galloway 2004, 11; Power 1990). In relation to my thesis, protocols that govern information networks are then also governing the flows.

Galloway instructs that protocol is totalizing; it produces universality from diversity (2004, 243). Following that line of argument, I posit that in the context of my thesis universality is the subject as object denuded of contextual sense. This I believe is

an inherent tension between the rhetoric of iSpaces and ambient intelligence in pervasive computing in which the distributed computing model is intended as a "context aware" system versus the reality of the mode of control necessary to organize the network. Sophisticated pervasive systems are then always bound by sets of rules that continually grow and adapt to govern new situations detected by input rather than truly 'sensing' activity in the environment. This is in keeping with Deleuze's theory that control is expressed as a modulation changing moment by moment (1995, 178).

If, as Galloway asserts, protocol has a totalizing effect, it means that the rules governing the flows do not tap into the content transported in the flows. This is not to say that the transport layer of the Internet cannot discern the packets of data being sent but rather that the *meaning* in the content is not analyzed.[55] The communication rules just send the packet of data dictated by conventions for transmission set out in protocols (Galloway 2004, 8). This also means that data of any kind can be organized and legitimized by the controls in accordance with the established transmission protocols and distributed along the pathways of the network.

Distributed systems organize the chaos of the flows which are in constant flux as new data is captured, dispersed, decoded and recoded and converted into "properties or events" (Bogard 2006b, 108). This idea is significant to the doppelganger effect. I assert that the rigid protocols governing the network organize sense as much as nonsense and thus can give rise to events and consequence that can be intentionally derived as much as unintended.

---

55 I will return to the structural elements of the Internet in more detail in Chapter Five in a discussion on codes and law.

In Chapter One, I invoked the common chaos theory metaphor of the butterfly effect. Chaos is an element in/of distributed systems in nature and in computing (Urry 2006). Chaos in distributed computing is an effect that can be mitigated by programming in a response to unpredictability such that a system is capable of approximating an outcome based on fluctuating or unexpected inputs (Ditto and Munakata 1995; Dhillon and Ward 2002). It bears mentioning here because the doppelganger effect itself is sensitive to initial conditions or inputs submitted to an analytic or inferencing engine for the purposes of profiling.

Chaos theory is applied in economic forecasting and market prediction, data encryption, information compression, network design and management; electronic circuit stabilization; cardiology; and consumer electronics and appliances (Ditto and Munakata 1995, 98). It follows a deterministic rule set from which unpredictable yet patterned results emerge to effect an event or condition (Urry 2006, 113). It is this odd formation of a kind of order out of chaos that governs distributed networks. Chaos theory suggests that seemingly small, insignificant perturbations or changes can effect large changes in a system and it is this occurrence that manifests in the doppelganger effect.

Databases as perfect writing machines

Computer science and its linear, rational approach to computational and organizational problems are based on the Cartesian tradition and follow the Enlightenment-era thinking of Hume and Kant that describe the world as divided into subjects and objects (Power 1993). Objects were then viewed as rigid and impermeable with properties that could not be extended beyond a category or class of objects in a

hierarchy (Power 1993). Philosophy and science have, over time, effectively challenged such rigid, categorical views. Computer science too has evolved beyond the hierarchical model of objects in a system of fixed categories. Objects in the contemporary computing model are assigned properties and can be separated into classes and clustered together and through analysis generate a diagram or map of relations, effectively producing information.

Databases can store any type of data on any person, place, or thing including information, sound, text, images, and transactions and interconnect with databases containing data on completely separate objects for the purposes of analysis (Dodge and Kitchin 2005b). The output of databases, the information and knowledge produced through analysis, is itself often contained in a new database. In this sense, databases have an iterative propensity in which successive inputs and outputs are reclassified, recategorized, and re-analyzed to resolve into other databases.

Databases are the framework for object relations where, "Knowledge in this context is a database of representations which can be translated into language" to describe reality (Power 1993, 2). It follows then that Poster's proposition of the database as language and thus the "perfect writing machine" describes the logic embedded in databases and its ability to *write out* identity from discrete personal facts captured and stored as data objects.

The DBMS provides the coherence for the model, or object relations, to function and is what moves data between databases and coordinates the analysis components. The DBMS is comprised of "business rules" and provides complex data analysis functionality

to generate "business intelligence" from data about individuals (or any subject) in an object-oriented environment (Yeung and Hall 2007). Through its very operation it reduces any subject to an object of analysis. DBMS are codes of control that structure the databases and coordinate the profiling function facilitating the input/output regime crucial to the reproduction of identity in the system. The DBMS can be thought of as productive in the same way as the database itself.

Individuals can *imagine* how they might be profiled but they cannot *know* precisely how personal facts are mapped within a profile generated by databases. The bits of data that comprise the digital doppelganger can be dispersed and re-enter the flows. The digital doppelganger, as the cluster of facts reassembled into an identity for profiling, can also be subsumed into other databases and re-circulate in the flows. In this way digital doppelgangers are reproduced *ad infinitum* in ways that are incomprehensible to the natural person until exposed by some event or directed query such as a credit check or passport application. Exposing the digital doppelganger exposes the doppelganger effect.

Digital doppelgangers are evidence of persistence as indeed is any profile or reproduced virtual identity. Persistence, as discussed in Chapter Two, suggests that data about individuals captured in databases has a habit of sticking around for a very long time. The flows themselves are a constant movement of data which persists and multiplies. Persistence, which can often result in out-dated and stagnant details being mired in a database for eternity, is not realized until it is made visible when the natural person is subject to actuarial analysis or submits to a security protocol. Data breaches or exposure also reveal digital doppelgangers. Such exposures and revelations clearly

illustrate what kind and quality of data is gathered by private and public sector bureaucracies.

Consequential outcomes

There is much focus on consumer surveillance and profiling (see Elmer 2004; Lyon 2001; Gandy 1993) as a proliferating aspect of contemporary life. Deeply embedded technologies, evident in the smart home example in Chapter Two, and increasingly embedded consumer practices continually produce personal data that includes personally-identifiable facts and personality-based details. The doppelganger effect suggests these contingencies have consequential outcomes for the individual. Individuals can make choices in the front-end interaction during an information transaction (shopping, banking or signing up on a website) to opt in or opt out of sharing certain information but the individual cannot participate in the 'backend' operations of the DBMS that fashion identity from their personal data through an analytical routine.[56]

Exposing the doppelganger effect requires exposing its attributes, its constituent parts, and its assembly. Where do traces of the doppelganger emerge? There are literally millions of instances of data exposure worldwide as a result of outright data theft by criminal effort; as high as 162 million records worldwide in 2007 (Erickson and Howard 2007; CBC 2008). Everything from stealing a wallet with credentialed identification,

56 See Elmer's point about the limits of the opt in/opt out approach (2004, 77-82). Often the individual is forced to trade personal information for services and/or product. Consent to data collection will be addressed in Chapter Five. In Chapter Five I will address data protection and informational privacy policy and approach in more detail but it is important to note that most consumer transactions in Canada that collect personal data are governed by the Personal Information Protection and Electronic Documents Act 2001 (PIPEDA). Very briefly, this *Act* dictates how and when and for what purpose private sector organizations can collect data.

banking and credit cards to sophisticated online breaches, phishing schemes and database hacking. Such exposures trigger digital doppelgangers.

Data is also exposed through public venues such as Facebook, email, YouTube and other personal and social media sites where it can be taken up for the purposes of fraud as easily as it can be subsumed by the insatiable appetite for news, gossip and intrigue (Solove 2007). The exposure of identity can manifest through the doppelganger effect as cases of mistaken identity and ruined reputation exacerbated by the ability of networks to disperse information, right or wrong, without verification.

Identity fraud flows from identity theft. I will offer a short explanation of these identity transgressions as a means to discussing the doppelganger effect in relation to this section's analysis of data breaches.[57] The Office of the Privacy Commissioner of Canada (OPC) defines identity theft as, "the unauthorized collection and use of your personal information, usually for criminal purposes" where criminal purposes are the fraudulent activities that result from the theft of identity details. As will become apparent in the examples below identity fraud or misidentification can also result by collecting and manipulating publicly available personal information.

Exposure and effect

In 2006 and 2007 two rather spectacular examples of data breaches occurred; spectacular by the number of individual records compromised as much as by the kind and type of information retained by both organizations. The first example concerns the theft of data from The TJX Companies, Inc. (TJX) a publicly-held US-based company that

57 Identity theft and fraud warrant a much fuller examination. An examination of the history and ascendancy of the issue seemingly exacerbated by contemporary digital technologies reveals many promising directions for future research (see Poster 2007; Solove 2007; Hoofnagle 2007).

owns a chain of retail stores in the US, Europe and Canada. Hackers, over the course of eighteen months in 2005-2006, breached electronic wireless security measures and accessed confidential credit and financial information on at least 45.7 million TJX customers (TJX.com 2007; CTV.ca 2007).[58]

Canada's Privacy Commissioner has produced a report on the TJX event highlighting the absence of sound data protection policies and weaknesses in the corporation's data security regime in addition to the type of data stored and the retention policies of the organization (OPC 2007). The OPC report detailed the records retained including credit card numbers, names, addresses and telephone numbers and driver's licenses or other provincial identification.

In the constellation of effects propagating the doppelganger effect, personal data and databases figure prominently. A breach of the magnitude of the TJX example highlights how much data can be stored within a large, multi-record database. Linking personal information to specific pieces of identification can provide the appearance of authenticity. In this case, name, address and telephone number along with date of birth (from the driver's license). The TJX data included identifying attributes alongside official government issued identification which increases the veracity or verifiability of the other personal information. In this instance credit card fraud may be unnecessary; rather, the identifying individual details can be used to apply for new credit or as part of creating a synthetic identity (Hoofnagle 2007; Solove 2007). Digital doppelgangers emerging from

58 Some media sources reported in October 2007 that the data breach is as high as 94.7 million records which far exceeds the original number disclosed by TJX and investigated by the OPC in their September 2007 report (CTV.ca 2007; OPC 2007); A class action suit by affected TJX customers has resulted in a negotiated settlement only just being formalized and implemented in February 2008 (TJX.com 2008).

the TJX breach will be accurate proxies able to act with some authenticity when reproduced by databases.

The second example concerns a breach of data security by a public sector organization in the United Kingdom. On October 18, 2007, two discs containing 7.25 million Child Benefit records, involving twenty-five million individuals, were lost en route between Her Majesty's Revenue and Customs (HMRC) ministry offices and the National Audit Office (BBC.co.uk 2007; UK Information Commissioner's Office (ICO) 2007). While there have been breaches by branches of Canadian government ministries, but nothing in the order of magnitude of the HMRC.[59]

The HMRC and the Government of the UK have data protection policies in place to govern the transfer of data whether by hand or by electronic means and these policies were not followed (UK Information Commissioner's Office (ICO) 2007). This instance involves detailed personal information collected by government and then collated in one multi-record database including: national insurance number; name, address and birth date; spousal details; names, sex and age of children; and bank account details (BBC.co.uk 2007).

This example is particularly interesting given the types of personal data stored together in one place and its veracity which, I suggest, will make future attempts at identity fraud easier as a precursor to the doppelganger effect. Government records are highly valued by unscrupulous data brokers by virtue of their authenticity; it is assumed

59 Nymity Inc. is a Canadian company which tracks and reports data breaches including cases such as Canada Post's accidental exposure of customer shipping information online; medical faxes mistakenly sent to non-confidential recipients; and lost medical records in New Brunswick (nymity.com 2008).

the records contain factual details verified by official applications for national identity documents and bank accounts (Ward 2007).

The two data breaches demonstrate a potential risk in data record-keeping due to the overall number of records stored together and the likelihood of data and/or database consolidation. Database consolidation, in which multiple records and/or multiple databases combine, is significant to the doppelganger effect. The consolidation of multiple records from multiple sources enables the database to write out very detailed individual profiles (Mitchell 1999; Hoofnagle 2007; Singel 2007). Consolidation also relates to synthetic identity theft in which multiple individual identity details are mixed with false facts to produce a new identity for the purposes of identity-based fraud (Hoofnagle 2007).

When such large amounts of data are exposed, individual instances of identity fraud will be difficult to trace, particularly if multiple data records are used to compile synthetic identities. It is too early to tell what exact outcomes, if any, will unfold flowing from the TJX and HMRC breaches but the doppelganger effect suggests that sophisticated identity fraud could emerge as a result. Digital doppelgangers reproduced from these incidences will pollute individual credit reports in ways that are increasingly difficult to challenge (Solove 2007, 18). The doppelganger effect suggests that codes of control such as the DBMS will add coherency to fraudulent activity stemming from the misuse of such a rich collection of personal information.

Data exposure illustrates the destabilizing influence of the doppelganger effect. Its potentiality disrupts data protection security efforts by inserting an added layer of fact-

checking and ongoing vigilance as each new instance of data exposure is revealed. The onus of watchfulness is often passed on to the consumer by government agencies such as privacy and information offices as well as by media reports. Individuals, however, cannot realistically intervene in data collection and storage practices and are often unaware of fraudulent activity impinging on their credit and financial status (Solove 2007).

Thus, one of the outcomes of the doppelganger effect is to solidify data protection and security standards and encourage preemptive data checking on the part of the individual consumer. The consumer is encouraged by both government and private sector organizations to check their own financial records and credit history. The effect of this preemption serves to verify details in private and public sector databases which benefits the bureaucratic collection strategies of both sectors (CIPPIC 2006).[60]

In this way data breaches encompass a rather odd paradox. The breaches reinforce the data-centric requirements of neoliberal forms of governance by shifting the focus to the individual and encouraging heightened practices of self-responsibility and accountability for information in databases. Corporations that have weak data security regimes may be compelled by law to address those weaknesses but the overall approach to data protection and informational privacy is not necessarily questioned. The fact remains that data is collected and companies should protect it but when they do not the individual is ever cast as the 'potential victim of fraud' and responsible in some way for giving away all the information in the first place.

However, the doppelganger effect principally attests to the power of databases to

60 In relation to the data brokerage industry the value and veracity of the personal information goes up with each instance of authentication (CIPPIC 2006).

reproduce identity in ways that are beyond the control of the individual. Data that is lost or stolen and re-used for fraudulent purposes is in no way contained by data protection policies. It is contained by code and code can be compromised. Databases, as the next examples will illustrate, amplify and lend a certain coherence to fraudulent or misdirected acts.

Indexing and amplification

In Daniel Solove's (2007) examination of reputation on the Internet he relates an incident of identity misidentification linked to the sexual assault case of Kobe Bryant, a National Basketball Association star player in the US. Mainstream media did not identify the alleged victim of the assault but speculation as to the victim's identity sprang up on the Internet (Solove 2007, 36; CNN.com 2003). By the actions of one or perhaps several individuals a young Denver area teenager was erroneously identified online as the sexual assault victim perhaps due to the similarity in age, appearance, name and geographic origin of the two women. Original images of the misidentified young woman were downloaded from her school's website and altered and superimposed in sexually explicit images involving Mr Bryant, often accompanied by salacious and fictitious statements about the young woman (thedenverchannel.com 2003). The incident exploded on the Internet with multiple instances and versions of the story appearing.

This incident relates more than the insensitivity and inappropriateness of the perpetrators who identified the wrong woman in the case and propagated the story. The effects that flowed from the initial misidentification circulated and proliferated precisely because of the way the organizing codes of control, the protocols, of the network operate.

An individual/s initiated the action but the network effects of the Internet amplified the event. The indexing functionality built into search engine technology such as Google and Yahoo! catalogue websites, keywords, and search results (Brin and Page 1999). Google relies heavily on 'cookies' which are small bits of code deposited on the user's computer linking them to sites they visit. In this way Google can link individuals with particular searches and to websites just as the websites can 'remember' the number of times the visitor linked to or visited a website (Gandy 2006, 374; see also Elmer 2004; Brin and Page 1999). This formula means that each 'hit' on the story, each search, each click on a link to a website report of it, pushes the incident higher in the rankings. This ensures the story will be located high up in a search query based on a keyword search. Each successive hit amplifies the problem.

Databases behind the search engines collect, sort, and analyze all search results. Social media sites that aggregate news stories based on their popularity tap into these results and generate their own sorted hierarchy based on viewer/user voting (businessweek.com 2005; reddit.com; digg.com). Each of these instances effectively promote a report and the links grow exponentially as more and more sites pick up the story. All rely on databases. It is not an individual engineering the cross-contamination of an unverified story but the architecture of the web itself that orchestrates the proliferation devoid factual authentication. In the Bryant example, personal information about the misidentified woman including her name, age, school, and address mixed with rumour and innuendo (Solove 2007). Her personal information was readily picked up in public sources and collated alongside incorrect information, resulting in the identity confusion.

The indexing and tracking that amplified this case could not be undone. It took television media to disseminate the real story and correct the misidentification which then percolated back into cyberspace (CNN.com 2003). The damage, however, is not undone by circulating the correction. The sordid tale can still be Googled. The false images persist. The misidentified young woman's digital doppelganger will linger in the archival apparatus of the Internet. This example is the doppelganger effect.

Intentional actions, unintended consequences

My final example of the doppelganger effect involves a short narrative describing what began as an intentional action resulting in an unintended consequence far beyond what any of the parties involved could have imagined. In 1989 a young Canadian medical student had her driver's license 'borrowed' without permission by her younger, under-age sister who, among several other more dubious uses, subsequently got a public library card using the 'borrowed' identification.

Fifteen years later the now successful doctor applied for a home mortgage and was refused in spite of her seemingly excellent credit history. After complaining to the bank and demanding an explanation for the mortgage financing refusal she was called in for a meeting. She had to report to the regional head office on the ninth floor of a business tower in the city centre. She was ushered into a small, sparsely furnished room in which sat a man in a dark suit with a thick file on the desk in front of him. He said, "The library just wants their books back."

This somewhat amusing anecdote caused immense frustration and embarrassment for the individual involved and in the end, because she could not verify her sister had

taken her identification years earlier, she had to pay for the books. The incident, the bank told her, would remain in her credit history and lower her overall standing. The doppelganger effect, having produced a digital doppelganger who liked to steal library books may regenerate another doppelganger in a different scenario because of the penchant for database consolidation among credit bureaus. The bank did give her the mortgage and in seven years her credit ranking will go back up.

This incident illustrates how personal data stored in one database and, either through cross-referencing or transfer, made its way into another database and reproduced a digital doppelganger containing historical facts without context and devoid of any verification. The identity profile generated by the bank's database was the proxy for an important life choice; yet its facts remained unverified until challenged by the individual refused a financial service. In the end it is the individual who must assume responsibility for correcting their profile and be accountable for its accuracy even as they have no control over how they have been or will be profiled in the future.

Conclusion

The doppelganger effect is the moment of record created by the "perfect writing machine" in a highly circumscribed discursive act which reproduces individual identity/ies *in absentia*. The natural person remains uninvolved in how, and in what manner, their identity is written out as an object of analysis. The capacity of the database to re-write the individual in innumerable ways without direct involvement, interaction, control, or input is the doppelganger effect.

The doppelganger effect is that moment of reproduction no matter how legitimate; a

moment beyond the control of the individual. The individual does not have authorial control over the identity reconstituted and the resulting analytical profile. Individuals cannot write the conclusion to the story of bits and pieces of their life captured in and extracted from databases; the information is re-cast according to external analytical criteria, parameters, actuarial variables, or credit requirements. It is the constellation of effects that culminate in the moment of analysis when the profiled emerge as a "knowable object" devoid of character but imbued with personality traits. The doppelganger effect encompasses the intended and the unintended consequential outcomes of identity reproduction, good and bad, positive and negative, appropriate or defective.

In the approach taken by poststructuralists in which identity management is bound to the productive and discursive power of the database, control can never manifest in the individual because they cannot understand the language of the database (Zwick and Dholakia 2004, 40). This position is an affront to established data protection and informational privacy policy to which I turn in the concluding chapter.

Chapter Five

Law Meets the Multiples of Cyberspace (Lex Meets Multiplex)

> With the dissemination of databases, a communications technology pervades the social space and multiplies the identity of individuals, regardless of their will, intention, feeling or cognition.[61]

In September 2007 I attended the 29th International Conference of Data Protection and Privacy Commissioners in Montreal, Canada. The keynote address was delivered by Mr Michael Chertoff, head of the U.S. Department of Homeland Security, who appeared only after the hotel hosting the event was 'locked down' and conference attendees had provided identification and registration details to gain entry to his address. U.S. Secret Service agents quietly but not unobtrusively patrolled the perimeter of the conference room, no doubt protecting all of us from the "enemies of freedom" who, apparently, also undermine privacy. It is, Chertoff argued, this "dark world of our adversaries" that forces the mandatory transferral of passenger flight data collected by commercial airlines to U.S. law enforcement agencies for the purposes of profiling. It is this procedure which generates the first stage of compiling the no-fly list for the U.S. government in a giant trade-off between privacy and security. Chertoff stressed that the data is now *only* retained for fifteen years down from the original forty.[62]

In a strange twist of fate I was seated during Chertoff's address next to the Chief Privacy Officer (CPO) for a large American corporation that provides networking and systems measurement services to the Department of Homeland Security (DHS) and other

---

61 Poster (1995, 68).

62 Chertoff's comments are taken from the opening address at the 29th International Conference of Data Protection and Privacy Commissioners in Montreal, Canada, September 25-28, 2007. A video of his address can be found here: <http://blog.privcom.gc.ca/index.php/2007/10/19/secretary-chertoff-speaks-on-privacy-and-security/>.

public and private sector organizations. For reasons he cannot and does not know he is on the second tier U.S. no-fly list which means he cannot take advantage of online check-in services for any airline and must check-in at the airport to undergo secondary screening. He has no information on why he is on the list nor specifically how to get himself off; he has no input into how he was profiled and how his identity was reproduced by the analytic engine within the profiling machinery of the DHS. What personal facts were drawn together to create his digital doppelganger such that it triggered inclusion on the no-fly list? The CPO's digital doppelganger will stand-in for him for at least three years but how can he prevent a recurrence if he does not know how his identity was reproduced?[63]

In this chapter I will bring together the ideas of the preceding four chapters to examine informational privacy and data protection approaches in view of my assertion that the doppelganger effect sets in motion consequential outcomes for the individual. As much as private and public sector organizations attempt to follow a regulatory framework and set of best practices to govern the collection, use and disclosure of personal information, this approach falls short of reducing the flows of data. It fails to address the multiple ways the individual is reproduced by databases. It cannot suppress the doppelganger effect.

I will not undertake a policy analysis of Canada's *Personal Information Protection and Electronic Documents Act* 2001 (PIPEDA), but rather an examination of whether the approach to privacy and data protection overall is appropriate given the protocols and

63 The DHS has a process to investigate misidentification accessed here: <http://www.dhs.gov/xtrvlsec/programs/gc_1169676919316.shtm>. The CPO was quoted a potential wait time of three years by DHS officials after submitting an application for redress, however, he will never be told why he ended up on the no-fly list.

distributed infrastructure of contemporary networks and their effect on the constitution of the subject. Two questions guide my analysis: firstly, how might the formal legal rules and regulations for privacy and data protection contain the multiples of cyberspace? Secondly, are such regulatory measures an "operable technical form" which aid neoliberal forms of governance (Rose 1993, 13)? The doppelganger effect, I will argue, is aided by the very practices meant to contain it and is exacerbated by the insatiable appetite for data required for contemporary neoliberal governmentality in which privacy is so often equated with security.

The data protection approach

Data protection and informational privacy is intended to balance the privacy interests of the individual with that of the state and private enterprise collecting personal data (Bennett and Raab 2003, 34). The approach endeavours to protect information about individuals through fair information principles (FIPs) and data privacy and protection policies and/or legislation. In Canada privacy is not a right guaranteed under the *Canadian Charter of Rights and Freedoms* (*Charter*) nor in the *Privacy Act* which protects private information collected by public sector institutions. It thus falls to PIPEDA, or similar provincial acts, to ensure that corporations safeguard personal information they collect.

PIPEDA is focused on protecting personally-identifiable data around the locus of informational privacy. Provinces that have legislated privacy acts, and/or freedom of information and protection of privacy statutes (FIPPAs), and/or personal information protection acts (PIPs), that meet the standards set out by PIPEDA are governed by their

own provincial legislation (Austin 2006). For the purposes of this discussion, I will refer to PIPEDA. The Office of the Privacy Commission of Canada (OPC) produces an annual report for submission to Parliament in which it outlines yearly complaints resolution and outcomes, current and future risks to data protection, and related Commission projects and research (privcom.gc.ca 2008). Overall, the OPC views PIPEDA as working "reasonably well."

Asymmetry and fuzzy reasonableness

Privacy advocates and legal scholars contributing to privacy research and policy analysis in Canada have, since PIPEDA's inception in 2001, been involved in ongoing reflection and critique of the *Act*. Analysts and scholars have critiqued the procedures and rules in the compliance and complaints provisions instituted under PIPEDA; the Act's data retention policies; and the unequal relationship between data collectors and the individual. The Canadian Internet Policy and Public Interest Clinic (CIPPIC) has been engaged actively on behalf of citizens to challenge PIPEDA's shortcomings and as such has initiated formal complaints to the OPC based on specific instances of corporate non-compliance. CIPPIC has also undertaken its own reviews of compliance to data protection laws by those Canadian corporations collecting personal data and among companies engaged specifically in data mining (2006a; 2006b; 2007). Their findings have exposed numerous failings among Canadian corporations to adhere to the provisions governing personal information laid out in PIPEDA.

It must be stated that while the OPC remains complaints-focused overall there is an effort by the OPC to publicize data protection and informational privacy by creating a

"privacy toolbox" for organizations to aid their compliance efforts (privcom.gc.ca/bus 2008). The OPC under Commissioner Jennifer Stoddart has been much more proactive than her predecessors toward privacy education and public awareness while at the same time increasing the OPC's procedural transparency (Berzins 2004; privcom.gc.ca 2008). On the surface these are positive efforts if considered as part of the mandate of the OPC to provide oversight for PIPEDA, but as I will later demonstrate the *Act* serves to reinforce particular goals in keeping with neoliberal strategies of "governing at a distance."

The OPC's mandate is "overseeing compliance" with PIPEDA in the private sector and with the *Privacy Act* in the public sector (privcom.gc.ca 2008). Central to the OPC is the investigation of complaints about corporate data handling practices, alleged privacy infractions, and PIPEDA compliance issues. Christopher Berzins (2004) provides an important criticism of the OPC's procedural format underpinning the complaints process. The OPC complaint's process is reactive; it receives a complaint and reacts by investigating. This complaints-driven process produces rules that "coalesce into agency policy" framed by the parties in dispute — such reactive policy-making can make the outcome linked to the kind and quality of complaint launched (Berzins 2004, 114).

Berzins' analysis raises a critical weakness of the data protection and informational privacy approach by highlighting what Jeanette Teh identifies as the "disparity of bargaining power" between organizations and individuals and the "lack of consumer knowledge" about data collection strategies deployed by corporations (2001, 23).[64] This

64 This echoes Elmer's argument that data collection forces individuals into choosing between disclosure in exchange for products and services or no disclosure and hence a refusal of products and services (2004, 6).

asymmetry in power can skew complaints results toward the more resourceful party and in cases where an OPC ruling is appealed to the Federal Court this can be an expensive undertaking. It suggests that the quality of complaints may be sensitive to the resources available among the parties to mount or defend actions relating to compliance which may favour well-funded organizations over individuals (Berzins 2004).

Teh also challenges the ambiguous language of PIPEDA in her critique. The *Act* considers what a "reasonable person" might find to be acceptable practices of data collection in electronic transactions that are increasingly more complex to define and in which the "reasonable person" is increasingly more diverse (Teh 2001). PIPEDA also refers to potential privacy-invasive situations or areas of oversight by suggesting "some information" may be collected but, as Teh points out, not specifically outlining *what* information would infringe on individual privacy. By emphasizing notions such as "reasonable expectation" and prefacing governable collection practices with indeterminate language such as "some information," PIPEDA creates more not less uncertainty for individuals engaged in commercial transactions requesting personal information.

Fully informed consent remains fuzzy under PIPEDA — a fact to which I will return in the subsequent section on privacy as data control. The *Act* does not provide clear guidelines for an organization's declaration of "identified purposes" for data collection and use making it difficult for individuals to make an informed choice when consenting to data collection (Teh 2001, 31). The onus throughout PIPEDA is on an organization's effort to be "reasonable" as regards data collection, use and disclosure but defining

"reasonable" is, as discussed, notoriously difficult to do. In fact, the use of the subjective term "reasonable" throughout PIPEDA creates the illusion of an objective standard when there is none (Teh 2001, 32).

PIPEDA is further limited by vague language in section 4.5 Principle 5 dealing with data retention. The *Act* deliberately uses the work "should" over "shall" stating that, "Organizations should develop guidelines and implement procedures with respect to the retention of personal information." (PIPEDA; see also Warner 2005). The use of "should" is more suggestive of a recommendation for data retention than an obligation with specific terms and limits for retention and, as argued by Jeremy Warner, significantly reduces the force of PIPEDA in this critical area (2005, 13). This has implications for the doppelganger effect as well. Data retention makes instances of the doppelganger effect more likely when long term file storage occurs alongside weak data protection measures as in the TJX data breach example.

From my point of view, these critiques do not address the policy's underlying form as a constitutive element in/of neoliberal governance nor the potential disconnect between the objectives of commerce to collect and use data and individual privacy goals. While constructive criticism and direct action by privacy advocates and analysts is important, for the purposes of my analysis I will trouble the underlying framework of data protection through the lens of the doppelganger effect. My critique will proceed along three lines: the presumption of commercial data collection as a basis to the framework; privacy as data control; and code (software) and law.

Commerce and control

Presumptive commerce: An Act to support and promote electronic commerce[65]

The presumption of commercial data collection threaded into data protection and informational privacy policy, including PIPEDA, is a problematic legitimation of corporate "dataveillance" (Clarke 1994; Bennett and Raab 2003; Barrigar 2006). From the outset commercial concerns have been part of the development of data protection policies. Development began with the European Union protection directive in 1990 and extended to the Canada Standards Association (CSA) Model Privacy Code released in 1996 as a framework for PIPIEDA (Bennett and Raab 2003, 168; Barrigar 2006, 14).[66] This commercial framework ensures that data protection policy will not curtail commerce and trade and at the same time drives data collection and security standardization between data collectors and between countries who comply with international data standards. Economic efficiency prevails over individual privacy in this model (Barrigar 2006, 32).

Data protection and informational privacy employ strong liberal language to construct the policy as one which puts control into the hands of the individual, or more accurately, the consumer, to make choices around disclosing personal information. However, in a system that takes as its starting point the fact of, the continuation of, data collection by commercial interests for the purposes of profiling, "privacy protection may be in danger of becoming absorbed into ... consumerism" (Raab 1999, 76). As I have

65 The opening statement of PIPEDA states: "An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances."

66 The CSA code forms the basis of Schedule 1 of PIPEDA and as such is an "an extremely unusual degree of private sector involvement in the actual drafting of the law" (Barrigar 2006, 14).

argued elsewhere, there are ongoing pressures to formally inaugurate the form of an electronic persona as property fully commodifying aspects of personality and intimate facts. Data protection and informational privacy may hasten this transformation.

Privacy as data control

The underlying framework for privacy, the privacy paradigm common to most Western liberal democracies, rests on the conception of a society made up of autonomous individuals. Privacy is conceived as a pre-condition of liberalism along with autonomy, rationality and liberty (Bennett and Raab 2003). It rests on John Stuart Mill's notion that the individual requires a place of repose to develop an "inward domain of consciousness" that only privacy permits and without it liberal subjects cannot properly be purposeful, autonomous agents ([1909] 1993). This is reflected by Joseph Kupfer's argument that privacy is a basic value required for the development of the autonomous self and that autonomy needs a "conception of self" only made possible through privacy (1987, 81). These conceptions suggest a spatial configuration of privacy as a "private sphere untouched by others" (Bennett and Raab 2003, 21).

By tracing the effects of surveillance and data collection and the implications for privacy and identity, the preceding chapters illustrated how attenuated the classic liberal privacy paradigm has become. Informational privacy and data protection has become a more dominant conception suited to the network society's space of flows supplanting or at least diminishing a spatial notion of privacy. However, informational privacy also remains grounded in basic liberal philosophy of the autonomous, self-choosing individual reflecting privacy as control over personal information (Allen 2000; Schwartz 2000).

The language of choice evident in liberal philosophy adopted by legislative as well as self-governing approaches to data protection and informational privacy under neoliberalism obscure the *conditions* of choice offered to the individual. The choice offered under the umbrella of informational privacy is whether or not to consent to data collection, use and disclosure; to opt-in or out of data collection most often in exchange for goods and services.

Greg Elmer (2004), in his examination of consumer profiling, highlights the complex back and forth between the individual consumer and corporate provider in which the consumer trades personal information for goods and services. The reasons individuals are seduced into this behaviour are complex. They may involve what Jennifer Barrigar *et al.* (2006) describe as social engineering of choice, and which social and cultural theory scholarship on profiling, choice, and consent frame as interpellation.[67] As discussed elsewhere in my thesis, this is the subtle action that entices individuals into acts of self-surveillance by giving away information about themselves (Poster 1996; Lyon 2003). It exists as part of a confluence of 'call and response,' or 'ask and receive,' amid the ongoing coercive process of neoliberal governmentality; a self-actualization that enables sophisticated social control packaged as choice by consent.

Privacy as data control acknowledges the deeply embedded liberal autonomy principle wherein the individual is positioned as a self-determining agent capable of controlling their own personal information (Schwartz 2000, 820). Privacy thus becomes

---

67 Barrigar *et al.* (2006) looks to "cognitive tendencies" that shape whether or not an individual consents or withdraws consent. The authors suggest that together "cognitive dissonance, prospect theory, and discounted subjective utility" can explain how individuals make choices around consent and data collection practices. As I suggest in the text there is extensive commentary on consumer behaviour in relation to surveillance and data collection to be found in surveillance studies and social and cultural theory in the work of Greg Elmer, David Lyon, Mark Poster and others referenced at different points in my thesis.

conflated with choice; the choice to consent to collection, use and disclosure of personal information is directed at protecting informational privacy. It becomes mired in the "autonomy trap" intended to make individuals feel like they are exercising control by being asked for their consent (Schwartz 2000, 828).

Data protection and informational privacy bundle control in a right shaped as both reducing harm to the individual (the protection part) and control over their personal information (the privacy part). Data standardization and procedural guidelines are promoted as good for the individual as a harm reduction strategy aimed at mitigating negative effects that accrue through collection, use and disclosure of personal data (Raab and Bennett 1996; Barrigar 2006). As I argue below, this claim can be undone by challenging what is really meant by 'use' conveyed through the consent process.

The objectifying analysis undertaken by corporations as part of their 'use' of the data cannot be actively governed by the individual. Data protection guidelines that govern collection, use, and disclosure do not transfer power post-collection back to the individual. In theory, consent can be withdrawn but in practice this does not reclaim privacy for the individual nor nullify existing profiles or digital doppelgangers.

The object of my critique is the overall approach to data protection and informational privacy which privileges information about individuals over and above individual privacy. Informational privacy places the self-choosing and self-managing individual as the preeminent *object* of regulation offering false choices that convey a sense of control over personal information and privacy.

Facts about individuals can be sorted, catalogued and constructed into virtual

representations – a reconstituted identity that ties who individuals are to facts, habits, and preferences abstracted from the natural person. Facts about individuals construct one identity in the virtual world where lived life looks very different than in the presence of contextualized habits and preferences of the material world. Informational privacy protects only data and information produced within the material world; it does not shelter the natural person and their "inviolate personality" from the multiples of cyberspace.

I argue that privacy as data control is a fallacy. What is the point of control if the individual cannot then control what sort of identity is reconstructed from their personal data? The analytical outcome has implications for the natural person in the material world whether it is a market profile, insurance forecast, or financial credit check. I argue that viable control, in the model projected through data policies, stops at the point of consenting to collection, use, and disclosure regardless of the regulatory regime. What matters to the individual is how identity is reformulated through the process of analysis and controlling the bits and pieces of data means nothing if the individual cannot control the conclusions or outcomes generated by the "perfect writing machine."

I argue that current approaches to informational privacy and data protection are ineffective given the productive power of code to dislodge the liberal subject at the centre of that model. This suggests a different frame and orientation to data protection and informational privacy is required that is not mired in the "autonomy trap."

Juridical intermediaries[68]

Nigel Thrift and Shaun French hold that software, and hence code, has an in-built power manifest through its ability to permit/not permit access to a place, product, space, or thing (2002). Software has become a "potent juridical intermediary" tightly bound to governance routines and rules of conduct for citizen-consumers (Thrift and French 2002, 325). It has truly extended the notion of "governing at a distance" by algorithm and calculation.

There should be no surprise, then, that an attraction between the law and the architecture and software of the network society, principally of the Internet, has coalesced. The language of software with its coded and bracketed strings and definitions, rules and procedures, maps to the procedural logic of legal regulation. In the context of data protection and informational privacy, data security and identity management are enabled by both the language and programming of credentials and trust welded to the permitted/not permitted binary logic of networks. It turns out that the very structure of the Internet, the networking infrastructure, lends itself to various models of Internet governance and regulation.

The Internet's architecture consists of several layers, depending on what networking model is deployed, and these layers provide a framework upon which to base legal rules for governing the Internet and flows of information. Technologists and social and legal analysts each have a particular way of viewing the technical aspects of the network

68 Thrift and French (2002, 325).

translated as layers.[69] For the purposes of my discussion and to minimize confusion and unnecessary complexity, I will refer to a pared down four-layer model referenced in Craig McTaggart's Internet legal analysis consisting of the physical, operational, application and content layers (2003). These four layers feature prominently in discussions of the legal and structural issues dominating Internet regulation.

Each of the layers of the Internet are expressed in code. Code, coded protocols and software rules determine how the global information flows are organized. Data is routed through and along the layers from the physical backbone or cables, modems and routers to the application layer from which computer servers 'serve' up or deliver web pages in the content layer to individual computers and digital devices (Blank 2002). The operational layer combines the transport and linking functionality relying on complex Internet protocols (IP) and the services of Internet Service Providers (ISPs) (McTaggart 2003; Blank 2002).

Internet protocols operate as traffic coordinators, in the most simplistic rendering, and facilitate the collection, connection, and transmission of data in, out, and around cyberspace; these codes or protocols organize the flows (Blank 2002; Galloway 2004). Alexander Galloway's work on analyzing protocols encompasses both Gilles Deleuze's control society concept and Manuel Castells' network society flows but with more specificity in seeking to define protocols that direct and structure the Internet as a "formal

69 Those of us with a background in information technology and network management tend toward the Open System Interconnection (OSI) reference model consisting of seven layers, but that model is, in my view, overly burdensome for the purposes of my discussion here. The OSI model provides a reference for other compressed models that often combine one or two layers. It starts at base with the physical layer and works 'up' to the application layer whereas other models combine the mid-layers and include content as a layer. The OSI model layers are: physical layer, data link, network, transport, session, presentation, and application (Blank 2002; Cisco.com 2006).

apparatus" (2004, 54, 64). Protocols, within the operational layer, are the codes of control that structure distributed networks and are thus culpable in the doppelganger effect.

Is code law?

Lawrence Lessig has been a defining voice in the debate around Internet regulation arguing that there is symmetry between the law and code. He has gone so far as to say that, "code is law" (Lessig 2006, 5). Lessig, while once championing free culture in the nascent anarchical days of the Internet now concedes that the Internet is governable; that it can be regulated and code is the operative technical means to do it (2004; 2006).[70]

Galloway notes that code and protocols which provide organizational control and coordination to the flows of information in the network society predate the formal notion of binding code to law (2004, 141). He argues that networks, and the Internet being the grandest of them all, have always operated under strict controls but it is the expansion and commercialization of the Internet which fertilized the idea a decade ago that it was ungovernable in a meaningful way (2004, 141). This fact, however, uncovers another relating to data protection and informational privacy. It is precisely the established and standardized protological controls developed historically without any consideration of privacy norms that make it difficult to now attach privacy enhancing principles and technology to the network architecture.

Code as law of the Internet could refer to any number of potential areas of regulation and Lessig comments on many in his book *Code 2.0* (2006), but his view on informational privacy is most relevant to this chapter. Lessig tilts toward information as

70 This is not to suggest that Lessig does not consider regulability with some caution and publicly supports the Open Source Software movement and other 'open' movements for sharing digital content such as through the Creative Commons initiative (2006; 2004).

property as a basis for protecting privacy (also discussed elsewhere in my thesis). Code in this configuration would govern access to personal information protected as property. Ultimately, a property right in personal information is seen as a way to mitigate against a future in which commercial interests alone limit the freedom of cyberspace (Lessig 2006; see also Wagner 2005, 460). It could balance the unequal bargaining power between organizations collecting data and the individual consenting to collection.

Lessig concedes that much opposition is aligned against his property proposal (see Schwartz 2000 and JE Cohen 2003) and suggests privacy-enhancing technologies (PETs) as another approach. PETs are technology-enabled solutions that embed privacy options or make privacy policy machine-readable to facilitate individual choice at the outset of a digital transaction (Lessig 2006, 230; w3.org/p3p 2007).[71] While this may seem a viable option, its adoption has been hampered by interoperability and implementation problems among Internet browser developers and by its complex set up and and user interface (w3.org/p3p 2007). Ironically, the PET approach would make property rights in information easier to enforce if it were adopted by enabling users to attach usage rights to personal information. This would blend Lessig's property approach to informational privacy-as-control with technology-enabled regulation.

Lessig proposes that PETs could be a new layer added to the infrastructure of the Internet as an "identity layer" sitting on top of the content layer (2006, 226). This would

---

71 Obligation specification language (OSL) is being tested as a possible model for enforcing privacy policies embedded into a document whereby the rights expression language component of the DRM system has privacy obligations embedded alongside it that govern the distributor and the consumer (Hilty *et al.* 2007, 538). While most of us are familiar with DRM attached to copyright music or video files, very similar tactics are used by organizations to protect trade secrets and confidential documents. A "distributed usage control" document access model based on OSL closely parallels DRM and uses an observation or reporting scheme to track content usage (Hilty *et al.* 2007).

entail using the Privacy Platform for Preferences (P3P) mechanism for appending computer-readable privacy policy and preferences to an identity (Lessig 2006, 226; see also w3.org/p3p 2007). The same issues and complications dog P3P as with PETs generally.

I argue that these solutions miss the point entirely. Controlling access would revolve around the same trade-offs present in consumer transactions requesting personal information in which information is exchanged for goods and services. This market-driven approach does nothing to reduce personal data collection and circulation; it does not address the ever-increasing presence of "dataveillance;" and it does not address how the individual is reproduced through the productive power of the database. If anything, PETs would enhance an already thriving trade in personal information.

Some years prior to Lessig's influential commentary on law and code, Joel Reidenberg identified a "rule regime" to govern information flow which he called "Lex Informatica" (1998). This influential model set out a regulatory regime that recognized that law and government were not the only source of rule-making in the "Information Society" but that technology and communications networks impose a set of rules on participants (Reidenberg 1998).

Reidenberg viewed his scheme as an enhancement of existing communications and regulatory policy and law. Lex Informatica would aid access, distribution and the use of information by setting up default rules which could be modified based on material law constraints. It also emphasized the case for self-regulation and voluntary compliance to fair information principles in the market but this, it turns out, has been a failure in

jurisdictions without legislated privacy protections (Litman 2000). However, Lex Informatica did chart relationships within the rule system between legal regulation and technological network elements across seven areas: framework, jurisdiction, content, source, customized rules, customization process and primary enforcement. The Lex Informatica features have at the very least set out a method and typology for subsequent examinations of Internet regulation and information flows.

So, is code law? Some legal scholars, such as Lessig and Reidenberg, would have us think so. Recent work by McTaggart (2003) and R. Polk Wagner (2005) also pursue this question with varying results. Wagner refines Lessig's "code is law" with "code meets law" (2005). He tweaks Lessig's dictum by reminding us that regulation by software is deeply embedded in commercial activities and practices that seek to regulate consumer behaviour. This is evident in consent practices governing data collection through consumer transactions and in the trade-off between digital media consumers and DRM systems enforcing license agreements.

Although legal scholars frame the discussion of code and law by relying on the layered infrastructure of the Internet, it is more explicitly the protocols coordinating the flows that provide a measure of control over the network itself. Galloway's "formal apparatus" of protocols invites parallels within law precisely because they are based on carefully constructed reference and specification documents and rule sets governing their architecture and functionality; they are codified much like law itself (2004). This protological formality, however, is not infallible in the sense that it organizes and routes

any and all kinds of information with maximum efficiency, regardless of legitimacy, as demonstrated in the Bryant example in Chapter Four.

Protological control is not regulation. But, I would argue, neither is code and, therefore, code is not law. Law is law and it may at times, in the context of information flows and contemporary distributed networks, demand formalized correspondence between the operational, application and content layers of the Internet to govern commercial relationships, data collection, informational privacy, and diverse communications. These points of connection and regulation are initiated in the material world to govern cyberspace. However, none of the proposals regarding regulation of personal information trouble the persistent collection and retention of data. There is no critique of the problematic instances of identity reproduction in which individuals are re-written by databases in a manner and form beyond their control. The "perfect writing machine" and its consequential outcomes continue to influence the life choices of individuals beyond the purview of regulatory instruments.

Conclusion

The approach to informational privacy and data protection under PIPEDA, founded as it is on the presumption of commercial data collection, is by design or accident, augmenting and extending the doppelganger effect by smoothing the collection of personal data. As a formal legal regulation it does more to facilitate the extension of collection practices in adherence to a set of norms and procedures *about* privacy rather than *protecting* privacy itself (Barrigar 2006). I argue that this is yet one more phenomenon in the constellation of effects that propagates the doppelganger effect by

legitimizing the collection of personal information without any consideration of the way in which individuals are then profiled.

The doppelganger effect challenges the more structured alliances that have taken form in the network society as proposals and instruments of control over the form and use of identity in cyberspace. Alliances evolving between government and the private sector developers of surveillance technology and data analysis systems and/or the informational assets produced by such systems. There are alliances between the coded rules or protocols of control coordinating the flows and formal legal approaches to defining and protecting virtual spaces, digital content, and digital personae. I argue there are implicit alliances between government agents such as privacy commissions and corporate organizations which drive standardization among data collection and storage practices that ultimately benefit bureaucratic systems of governance and not the individual. It can even be argued that the digital personae produced through profiling and analysis represent the organization of the subject by data analyzers into a formal model rendered as an object of commerce.

These alliances adhere to neoliberal governmental practices whose tendrils of influence and control embed into daily practices of information volunteerism and forced extraction in a willing population of self-managing citizens. Data protection and informational privacy policies fit this mode of governing by ensuring a steady stream of increasingly accurate and secure data aligned to standardized collection, security and storage practices. The emphasis on the self-managing individual interleaves responsibility and accountability and, in the context of my thesis, suggests that issues that arise from

ubiquitous data collection will always be the problem of the individual and not with the ever-increasing sites and technologies of surveillance. The self-actualizing and self-responsible citizen-subject is detached at the point of data collection from any meaningful control over their personal information – the individual can determine neither what happens to their data post-collection nor, as I have stressed, how they are profiled.

The consequential outcomes of "perfect writing machines" become visible to the natural person when they bump up against their digital doppelganger as proxy during what are often important life choices and decisions. They may apply for insurance and receive it without delay in which case their doppelganger looks pretty good. Conversely, the individual may apply for credit and be refused. In this instance, the individual sees the doppelganger and a decidedly uncanny image is reflected back; the facts and details that comprise the digital doppelganger look nothing like the self in the material world. These profiles can be reproduced contemporaneously looking radically different in each instantiation, but in any case the individual has no control over how their identity is written out by the corporate database seeded with objectified facts and indicia from life in the material world. The doppelganger effect is a new form of resistance within the network society; it resists unity of purpose with multiplicity and diversity. There is no 'one' out there, only the multiples and the many ones of cyberspace reproduced *in absentia.*

Bibliography

Abell, Peter and Diane Reyniers. 2000. "On the Failure of Social Theory." *British Journal of Sociology* 51 (4): 739–750.

Acquisti, Alessandro. 2004. "Darknets, DRM, and Trusted Computing: Economic Incentives for Platform Providers." <http://web.si.umich.edu/tprc/papers/2004/357/TPRC.pdf> (5 July 2007).

Adorno, Theodor. [1974] 2005. *Minima Moralia: Reflections from Damaged Life.* <http://www.marxists.org/reference/archive/adorno/1951/mm/ch01.htm> 9 January 2008.

Alexander, Bryan N. 1997. "Dialectical Nightmares: The Historicity of the Romantic-Era Doppelganger in the Works of Godwin, Hogg, Blake, Burney, and The Shelleys." PhD. diss. The University of Michigan.

Allen, Anita L. 2000. "Privacy as Data Control." *Connecticut Law Review* 32: 861-875.

------. 2001. "Coercing Privacy." *William & Mary Law Review* 40: 723-757.

Allon, Fiona. 2004. "An Ontology of Everyday Control." In *Mediaspace: Place, Scale and Culture in a Media Age.* Ed. Nick Couldry and Anna McCarthy. London and New York: Routledge.

Anderson, Nate. EU wants to slash search data retention period to six months. 7 April 2008 <http://arstechnica.com/news.ars/post/20080407-eu-issues-tough-data-protection-finding.html> (11 April 2008).

Andrejevic, Mark. 2002. "The Kinder, Gentler Gaze of Big Brother: Reality TV in the Era of Digital Capitalism." *New Media Society* 4: 251-270.

------. 2005 "The Work of Watching One Another: Lateral Surveillance, Risk, and Governance." *Surveillance & Society* 2 (4): 479-497.

Article 29 Data Protection Working Party. Opinion on Data Protection Issues Related to Search Engines. 4 April 2008 <http://www.cbpweb.nl/downloads_int/Opinie%20WP29%20zoekmachines.pdf> (11 April 2008).

Ball, Kirstie. 2006. "Organization, Surveillance and the Body: Towards a Politics of Resistance." In *Theorizing Surveillance: The Panopticon and Beyond.* Ed. David Lyon. Portland, OR: Willan Publishing.

Barnes, J.A. and F. Harary. 1983. "Graph Theory in Network Analysis." *Social Networks* 5: 235-244.

Barrigar, Jennifer. 2006. "Is You Is Or Is You Ain't: Making PIPEDA's Rights Language Meaningful By Re-Viewing Social Value." Unpublished draft cited by permission.

Barrigar, Jennifer, Jacquelyn Burkell and Ian Kerr. 2006. "Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information." forthcoming in *Canadian Journal of Business Law* <http://idtrail.org/content/view/349/42/> (9 March 2008).

Bartlett, Lexey Anne. 2005. "The Double Redux: Multiplying Identity in Postmodernist Identity." Ph.D. diss. The University of Texas at Arlington.

Baudrillard, Jean. 1988. *Selected Writings.* Ed. Mark Poster. Stanford: Stanford University Press.

BBC.co.uk. UK's Families Put on Fraud Alert. 20 November 2007. <http://news.bbc.co.uk/2/hi/uk_news/politics/7103566.stm> (21 November 2007).

Bermond, J.C., C. Delorme and J.J. Quisquater. 1986. "Strategies for Interconnection Networks: Some Methods from Graph Theory." *Journal of Parallel and Distributed Computing* 3: 433-449.

Bennett, Colin J. and Charles D. Raab. 2003. *The Governance of Privacy: Policy Instruments in Global Perspectives.* Aldershot and Burlington: Ashgate.

Berzins, Christopher. 2004. "Three Years Under the PIPEDA: A Disappointing Beginning." *Canadian Journal of Law and Technology* 3 (3): 113-126.

Bishop, Todd. Microsoft Home Pushes Boundaries of the Future. 28 September 2006. <http://seattlepi.nwsource.com/business/286739_msfthome28.html> (2 February 2008).

Blank, Andrew G. 2002. *TCP/IP Jumpstart: Internet Protocol Basics.* Alameda, CA: Sybex.

Bogard, William. 2006a. "Welcome to the Society of Control: The Simulation of Surveillance Revisited." In *The New Politics of Surveillance and Visibility.* Ed. Kevin D. Haggerty and Richard V. Ericson. Toronto: University of Toronto Press.

------. 2006b. "Surveillance Assemblages and Lines of Flight." In *Theorizing Surveillance: The Panopticon and Beyond.* Ed. David Lyon. Portland, OR: Willan Publishing.

Boling, Patricia. 1996. *Privacy and the Politics of Intimate Life.* Ithaca and London: Cornell University Press.

Boyle, James. 2002. "Fencing Off Ideas: Enclosure and the Disappearance of the Public Domain." *Daedalus* 131 (2); 13-26.

Bradley, Larry. 2007. Chaos & Fractals: The Butterfly Effect. <http://www.pha.jhu.edu/~ldb/seminar/butterfly.html>. (2 September 2007).

Brazil. 1985. Directed by Terry Gilliam [DVD]. Embassy International Pictures (Criterion Collection).

Brin, Sergey and Lawrence Page. 1999. The Anatomy of a Large-Scale Hypertextual Web Search Engine. <http://infolab.stanford.edu/~backrub/google.html> (4 December 2007).

Bull, P., R. Limb and R. Payne. 2006. "Pervasive Home Environments." In *Intelligent Spaces: The Application of Pervasive ICT.* Ed. Alan Steventon and Steve Wright. London: Springer.

Burk, Dan L. 2005. "Legal and Technical Standards in Digital Rights Management Technology." Minnesota Legal Studies Research Paper No. 05-16. <http://ssrn.com/abstract=699384> (10 January 2007).

BusinessWeek. "How Digg Goes Deep: The Collective Wisdom of the Web." 21 November 2005. <http://www.businessweek.com/magazine/content/05_47/b3960423.htm> (2 March 2008).

Cameron, Alex. 2004. "Infusing Privacy Norms in DRM: Incentives and Perspectives from Law." In *Information Security Management, Education and Privacy: IFIP 18th World Computer Congress, TC11 19th International Information Security Workshops.* Ed. Yves Deswarte, *et al.* Norwell, MA and Dudrecht, NL: Kluwer.

Castells, Manuel. 1996. *The Rise of the Network Society.* Cambridge, MA: Blackwell Publishers.

------. 1997. *The Power of Identity.* Cambridge, MA: Blackwell Publishers.

------. 2004a. "Informationalism, Networks, and the Network Society: A Theoretical Blueprint." In *The Network Society: A Cross Cultural Perspective.* Ed. Manuel Castells. Cheltenham, UK and Northampton, MA: Edward Elgar.

------. 2004b. "Space of Flows, Space of Places: Materials for a Theory of Urbanism in the Information Age." In *The Cybercities Reader.* Ed. Stephen Graham. London and New York: Routledge.

CBC.ca. Protecting Your Personal Information. 18 Febuary 2005. <http://www.cbc.ca/news/background/computer-security/phishing.html> (5 September 2007).

CBC.ca. Checking Your Credit Rating. 19 January 2007. <http://www.cbc.ca/news/background/identity-theft/credit-rating.html> (5 September 2007).

CBC.ca. Personal Data Theft Reaches Record Levels in 2007: Group. 2 January 2008. <http://www.cbc.ca/money/story/2008/01/01/data-theft.html> (10 March 2008).

Canadian Internet Policy and Public Interest Clinic (CIPPIC). 2006a. "On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship" A Report on the Canadian Data Brokerage Industry. April 2006. <http://www.cippic.ca/documents/May1-06/DatabrokerReport.pdf> (12 May 2007).

CIPPIC. 2006b. "Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up? April 2006. <http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf> (12 May 2007).

CIPPIC. 2007. "Digital Rights Management and Consumer Privacy: An Assessment of DRM Applications Under Canadian Privacy Law." September 2007. <http://www.cippic.ca/bulletin/> (29 September 2007).

Chertoff, Michael. 2007. Opening Address. 29th International Conference of Data Protection and Privacy Commissioners in Montreal, Canada, September 25-28, 2007 <http://blog.privcom.gc.ca/index.php/2007/10/19/secretary-chertoff-speaks-on-privacy-and-security/> (29 February 2008).

Cisco.com. Internetworking Basics. 2006. <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm#wp1020605> (25 March 2008).

Clarke, Roger. "The Digital Persona and its Application to Data Surveillance." 1994. <http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html > (8 March 2007).

CNN.com. American Morning: Discussion with Woman Wrongly Identified As Kobe Bryant's Accuser. 31 July 2003. <http://transcripts.cnn.com/TRANSCRIPTS/0307/31/ltm.05.html> (22 October 2007).

Cohen, Jean. 2002. *Regulating Intimacy: A New Legal Paradigm.* Princeton and Oxford: Princeton University Press.

Cohen, Julie E. 2000. "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review* 52 (5): 1373-1438.

-------. "DRM and Privacy." 2003. *Berkeley Technology Law Journal.* <http://www.law.berkeley.edu/institutes/bclt/drm/papers/cohen-drmandprivacy-btlj2003.html> (5 January 2007).

Critical Art Ensemble (CAE). *The Electronic Disturbance.* Brooklyn: Autonomedia. <http://www.critical-art.net/books/ted/index.html> (9 December 2007).

de Cauter, Lieven. 2004. "The Capsule and the Network: Notes Toward a General Theory." In *The Cybercities Reader.* Ed. Stephen Graham. London and New York: Routledge.

Davidoff, Scott *et al.* 2006. "Principles of Smart Home Control." In *Ubicomp 2006.* Ed. P. Dourish and A. Friday. Berlin: Springer-Verlag.

DeLanda, Manuel. 2002. *Intensive Science and Virtual Philosophy.* London, UK and New York, NY:Continuum.

Deleuze, Gilles and Felix Guattari. 1987. *A Thousand Plateaus: Capitalism and Schizophrenia.* Trans. Brian Massumi. Minneapolis, MN: University of Minnesota Press.

Deleuze, Gilles. 1995. *Negotiations*. Trans. Martin Joughin. New York: Columbia University Press.

TheDenverChannel.com. Woman Pictured As Kobe's Accuser Speaks Out. 30 July 2003. <http://www.thedenverchannel.com/sports/2368389/detail.html> (25 October 2007).

Dhillon, Gurpreet and John Ward. 2002. "Chaos Theory as a Framework for Studying Information Systems." *Information Management Resources Journal* Apr-June: 5-13.

Ditto, William and Toshinori Munakata. 1995. "Principles and Applications of Chaotic Systems." *Communications of the ACM* 38 (11): 96-102.

Dodge, Martin and Rob Kitchin. 2005a. "Code and the Transduction of Space." *Annals of the Association of American Geographers* 95 (1): 162-180.

------. 2005b. "Codes of Life: Identification Codes and the Machine-readable World." *Environment and Planning D: Society and Space* 23: 851-881.

Electronic Frontier Foundation. Sony BMG Litigation Info. 2006. <http://www.eff.org/cases/sony-bmg-litigation-info> (10 January 2007).

Elmer, Greg. 2004. *Profiling Machines: Mapping the Personal Information Economy.* Cambridge, MA and London, UK: The MIT Press.

Erikson, Kris and Philip Howard. 2007. "A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records." *Journal of Computer-Mediated Communication* 12 (4). <http://jcmc.indiana.edu/vol12/issue4/erickson.html> (12 November 2007).

Feelders, A., A. Daniels, and M. Holsheimer. 2000. "Methodological and Practical Aspects of Data Mining." *Information & Management* 37: 271-281.

Feigenbaum, Joan, *et al.* 2001. "Privacy Engineering for Digital Rights Management Systems." Security and Privacy in Digital Rights Management: ACM CCS-8 Workshop DRM 2001, Philadelphia, PA, USA.

Fisher, Ken. 2007. "Apple Hides Account Info in DRM-free Music, Too." <http://arstechnica.com/news.ars/post/20070530-apple-hides-account-info-in-drm-free-music-too.html> (15 September 2007).

Foucault, Michel. [1977] 1995. *Discipline and Punish: The Birth of the Prison.* New York: Vintage Books.

------. 1980. *Power/Knowledge: Selected Interviews and Other Writings 1972-1977.* Ed./Trans. Colin Gordon *et al.* Brighton, UK: Harvester Press.

Freud, Sigmund. 1919. "The Uncanny." Trans. San Diego State University. <http://www.williams.edu/go/Religion/courses/Rel301/reading/text/uncanny.html> (29 November 2007).

Galloway, Alexander. 2004. *Protocol: How Control Exists After Decentralization.* Cambridge, MA and London, UK: The MIT Press.

Galloway, Alexander and Eugene Thacker. 2004. "Protocol, Control, and Networks." *Grey Room* 17: 6–29

Gandy, Oscar Jr. 1989. "The Surveillance Society: Information Technology and Bureaucratic Social Control." *Journal of Communication* 39 (3): 61-76.

------. 1993. *The Panoptic Sort: A Political Economy of Personal Information* Boulder, CO: Westview Press.

------. 2006. "Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment." In *The New Politics of Surveillance and Visibility*. Ed. Kevin D. Haggerty and Richard V. Ericson. Toronto: University of Toronto Press.

Geist, Michael. 2005. "Copyright and Privacy: Through the Technology Lens." *The John Marshall Review of Intellectual Property Law* 4: 242-265.

Goffman, Erving. 1997. *The Goffman Reader*. Ed. Charles Lemert and Ann Branaman. Malden, MA and Oxford, UK: Blackwell Publishers Inc.

Graham, Stephen and David Wood. 2003. "Digitizing Surveillance: Categorization, Space, Inequality." *Critical Social Policy* 23: 227-248.

Haggerty, Kevin D. and Richard V. Ericson. 2000. "The Surveillant Assemblage."*British Journal of Sociology* 51 (4): 605-622.

Hay, James. 2000. "Unaided Virtues: The (Neo-)Liberalization of the Domestic Sphere." *Television and New Media* 1 (1): 53-73.

Heath, Pam and Nancy Bell. 2006. "The Changing World of Home Technology: A Microsoft Case Study." *The Information Society* 22: 251-259.

Hernandez, Michael J. 2003. *Database Design for Mere Mortals: A Hands-On Guide to Relational Database Design*. Boston, MA: Addison-Wesley.

Hilty, M. *et al.* 2007. "A Policy Language for Distributed Usage Control." Ed. J. Biskup and J. Lopez. ESORICS 2007, LNCS 4734: 531–546.

Hoofnagle, Chris J. 2007. "Identity Theft: Making the Known Unknowns Known." *Harvard Journal of Law & Technology* 21 (1): 97-122.

Howell, Robert G. 1998. "Publicity Rights in the Common Law Provinces of Canada." *Loyola of Los Angeles Entertainment Law Journal* 18: 487-509.

Information Commissioner's Office, United Kingdom. <http://www.ico.gov.uk/upload/documents/pressreleases/2007/helpline.pdf> (23 November 2007).

Intille, Stephen. 2002. "Designing a Home of the Future." *Pervasive Computing*: 76-82.

Jonker, H.L. *et al.* 2004. "Security Aspects of DRM Systems." Presented at the 25th Symposium on Information Theory in the Benelux, Roldue, Kerkrade, The Netherlands, 2-4 June 2004. <http://www.win.tue.nl/wic2004/23.pdf> (3 January 2008).

Jonker, Willem. 2007. "An Introduction to Digital Rights Management Systems." In *Security, Privacy,and Trust in Modern Data Management*. Ed. Willem Jonker and Milan Petkovic. Berlin, Heidleberg, New York: Springer-Verlag.

Kahn, Jonathan. 2003. "Privacy as a Legal Principle of Identity Maintenance." *Seton Hall Law Review* 33: 371-410.

Kerr, Ian. 2005. "If Left To Their Own Devices: How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy." In *In the Public Interest: The Future of Canadian Copyright Law.* Ed. Michael Geist. Toronto: Irwin Law.

Kerr, Ian and Jane Bailey. 2004. "The Implications of Digital Rights Management for Privacy and Freedom of Expression." *Information & Communication Ethics in Society* 2 (1): 87-97.

Kiel, Douglas L. and Euel Elliott. 1996. *Chaos Theory in the Social Sciences: Foundations and Applications*. Ann Arbor, MI: The University of Michigan Press.

Koch, Fernando L. and Carlos B. Westphall. 2001. "Decentralized Network Management Using Distributed Artificial Intelligence." *Journal of Network and Systems Management* 9 (4): 375-388.

Kupfer, Joseph. 1987. "Privacy, Autonomy and Self." *American Philosophical Quarterly* 24: 81-89.

Labriola, Patrick. 2002. "Edgar Allan Poe and E. T. A. Hoffmann: The Double in 'William Wilson' and 'The Devil's Elixirs'." *International Fiction Review* 29 (1,2).

Lessig, Lawrence. 2002. "Privacy as Property." *Social Research* 69: 247-269.

------. 2004. *Free Culture. How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York: The Penguin Press.

------. 2006. *Code: Version 2.0*. New York: Basic Books.

Lipton, Jacqueline. 2004. "Information Property: Rights and Responsibilities." *Florida Law Review* 56: 135-193.

Litman, Jessica. 2003. "Information Privacy/Information Property." *Stanford Law Review* 52 (5): 1283-1313.

Lorenz, Edward. 1963. "Deterministic Nonperiodic Flow." *Journal of the Atmospheric Sciences* 20 (2): 130-141.

Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham, UK and Philadelphia, PA: Open University Press.

------. 2002. "Everyday Surveillance: Personal Data and Social Classifications." *Information, Communication & Society* 5 (2): 242–257.

------, 2003a. "Surveillance as Social Sorting: Computer Codes and Mobile Bodies." In *Surveillance as Social Sorting*. Ed. David Lyon. London, UK and New York: Routledge.

------. 2003b. "Surveillance Technology and Surveillance Society." 2003. In *Modernity and Technology*. Ed. Thomas J. Misa, Philip Brey, and Andrew Feenberg. Cambridge, MA: The MIT Press.

Mackenzie, Adrian. 2002. *Transductions: Bodies and Machines at Speed*. London, UK and New York: Continuum.

------. 2005. "The Problem of the Attractor A Singular Generality between Sciences and Social Theory." *Theory, Culture & Society* 22 (5): 45-65.

Marx, Gary T. 2006. "Varieties of Personal Information as Influences on Attitudes Towards Surveillance." In *The New Politics of Surveillance and Visibility*. Ed. Kevin D. Haggerty and Richard V. Ericson. Toronto: University of Toronto Press.

------. 2001. "Murky Conceptual Waters: The Public and the Private." *Ethics and Information Technology* 3: 157–169.

Mell, Patricia. 1996. "Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness." *Berkeley Technology Law Journal* 11(1): 1-92.

McNairn, Colin and Alexander Scott. 2001. *Privacy Law in Canada*. Markham, ON: Butterworths.

McTaggart, Craig. 2003. "A Layered Approach to Internet Legal Analysis." *McGill Law Journal* 48: 571-625.

Microsoft Corporation. Microsoft Home Showcases New Prototypes of Technology for Daily Living. 28 September 2006. <http://www.microsoft.com/presspass/press/2006/sep06/09-28NewPrototypesPR.mspx> (26 February 2008).

Microsoft Corporation. Digital Rights Management (DRM). October 2005. <http://www.microsoft.com/windows/windowsmedia/forpros/drm/faq.aspx#drmfaq_1_4> (3 February 2008).

Mill, John Stuart. [1909] 1993. "On Liberty." >http://www.constitution.org/jsm/liberty.htm> (5 March 2007).

Miller, Karl. 1985. *Doubles: Studies in Literary History*. Oxford, UK: Oxford University Press.

MIT House_n. House_n Project Introduction. <http://architecture.mit.edu/house_n/intro.html> (22 February 2008).

Mitchell, William J. 2003. *Me++: The Cyborg Self and the Networked City*. Cambridge, MA and London, UK: The MIT Press.

Moore, Adam. 2003. "Privacy: Its Meaning and Value." *American Philosophical Quarterly* 40 (3): 215-227.

Morley, David. 2001. "Belongings: Place, Space and Identity in a Mediated World." *European Journal of Cultural Studies* 4: 425-448.

------. 2003. "What's Home Got To Do With It?" *European Journal of Cultural Studies* 6 (4): 435-458.

Nimmer, Melville B. 1954. "The Right of Publicity." *Law and Contemporary Problems* 19, no. 2: 203-223.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79 (1): 119-158.

Office of the Privacy Commissioner of Canada (OPC). Protecting Your Privacy on the Internet: Canada's New Privacy Law. 25 July 2004. <http://www.privcom.gc.ca/fs-fi/02_05_d_13_e.asp> (8 September 2007).

OPC. Identity Theft: Submission Presented to the Standing Committee on Access to Information, Privacy and Ethics. 8 May 2007. <http://www.privcom.gc.ca/parl/2007/sub_070508_e.asp#007> (12 November 2007).

OPC and the Office of the Information and Privacy Commissioner of Alberta. Report of an Investigation into the Security, Collection and Retention of Personal Information: TJX Companies Inc. and Winners Merchant International L.P. 25 September 2007. <http://www.privcom.gc.ca/cf-dc/2007/TJX_rep_070925_e.asp> (3 October 2007).

Patterson, Thomas C. 2005. "The Turn to Agency: Neoliberalism, Individuality, and Subjectivity in Late-Twentieth-Century Anglophone Archaeology." *Rethinking Marxism: A Journal of Economics, Culture & Society* 17 (2): 373-384.

Poster, Mark. 1996. "Databases as Discourse; or, Electronic Interpellation." In *Computers, Surveillance, and Privacy.* Ed. David Lyon and Elia Zureik. Minneapolis, MN and London, UK: University of Minnesota Press.

------. 2001. *The Information Subject.* Amsterdam: G&B Arts International.

------. 2007. "The Secret Self: The Case of Identity Theft." *Culture Studies* 21 (1): 118-140.

Pottage, Alain. 2002. "Unitas Personae: On Legal and Biological Self-Narration." *Law and Literature* 14 (2): 275-308.

Powell, Gavin. 2006. *Beginning Database Design and Implementation.* Indianapolis: Wiley.

Power, June. 1990. "Distributed Systems and Self-organization." Presented at proceedings of the 1990 ACM Annual Conference on Cooperation, Washington, DC: ACM Press.

------. 1993. "The Object in Perspective." *ACM SIGPLAN OOPS Messenger* 4 (2): 28-32.

Prosser, William. 1960. "Privacy." *California Law Review* 48: 383-423.

Raab, Charles D. 1999. "New Directions for Data Protection." In *Visions of Privacy: Policy Choices for the Digital Age*. Ed. Rebecca A. Grant and Colin J. Bennett. Toronto: University of Toronto Press.

Raab, Charles D. and Colin J. Bennett. 1996. "Taking the Measure of Privacy: Can Data Protection Be Evaluated?" *International Review of Administrative Sciences* 62: 535-556.

Radin, Margaret Jane. 1982. "Property and Personhood." *Stanford Law Review* 34: 957-1015.

Ranald, Ralph and Margaret Ranald. 1961. "Shelley's Magus Zoroaster and the Image of the Doppelgänger." *Modern Language Notes* 6 (1): 7-12.

Rank, Otto. 1971. *The Double: A Psychoanalytic Study*. Chapel Hill, NC: The University of North Carolina Press.

Regan, Priscilla. 2003. "Privacy and Commercial Use of Personal Data: Policy Developments in the United States." *Journal of Contingencies and Crisis Management* 11 (1): 12-18.

Reidenberg, Joel. 1998. "Lex Informatica: The Formulation of Information Policy Rules Through Technology." *Texas Law Review* 76 (3): 553-593.

Reiter, Eric. 2002. "Personality and Patrimony: Comparative Perspectives on the Right to One's Image." *Tulane Law Review* 76: 673-726.

Riva, G. *et al.* 2005. *Ambient Intelligence*. Amsterdam: IOS Press.

Rogers, Yvonne. 2006. "Moving on from Weiser's Vision of Calm Computing: Engaging UbiComp Experiences." Ubicomp 2006, LNCS 4206: 404-421.

Rose, Nikolas. 1993. "Government, Authority and Expertise in Advanced Liberalism." *Economy and Society* 22 (3): 283-299.

------. 2000. "Government and Control." *British Journal of Criminology* 40: 321-339.

Samuelson, Pamela. 2000. "Privacy as Intellectual Property?" *Stanford Law Review* 52 (5): 1125-1173.

Schoeman, Ferdinand D. 1992. *Privacy and Social Freedom*. Cambridge, Mass.: Cambridge University Press.

Schwartz, Paul M. 2000. "Internet Privacy and the State." *Connecticut Law Review* 22: 815-859.

Seleznyov, A., M.O. Ahmed and S. Hailes. 2006. "Co-operation in the Digital Age: Engendering Trust in Electronic Environments." In *Intelligent Spaces: The Application of Pervasive ICT*. Ed. Alan Steventon and Steve Wright. London: Springer.

Shapiro, William and Radek Vingralek. 2002. "How to Manage Persistent State in DRM Systems." DRM 2001, LNCS 2320: 176–191.

Singel, Ryan. Identity Theft Not Down, It's Different, Expert Says. 20 February 2007. <http://blog.wired.com/27bstroke6/2007/02/identity_theft_.html> (November 12 2007).

Sokal, Alan and Jean Bricmont. 1998. *Fashionable Nonsense: Postmodern Intellectuals' Abuse of Science.* New York: Picador.

Solove, Daniel. 2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet.* New Haven, CT and London, UK: Yale University Press.

Soppera, A. and T. Burbridge. 2006. "Maintaining Privacy in Pervasive Computing." In *Intelligent Spaces: The Application of Pervasive ICT.* Ed. Alan Steventon and Steve Wright. London: Springer.

Spigel, Lynn. 2001. "Media Homes, Then and Now." *International Journal of Cultural Studies* 44 (4): 385-411.

------. 2005. "Designing the Smart House: Posthuman Domesticity and Conspicuous Production." *European Journal of Cultural Studies* 8 (4): 403-426.

Stefik, Mark. 2007. "DRM Inside: DRM and the Future of Digital Media." Presented at keynote panel at Jupiter Media Digital Rights Strategies Conference. 17 September 2007; New York; NY. <http://www.parc.com/research/publications/details.php?id=6250> (2 November 2007).

Stalder, Felix. 2002. "Privacy is Not the Antidote to Surveillance." *Surveillance & Society* 1 (1); 120-124.

Teh Jeanette. 2001. "Privacy Wars in Cyberspace: An Examination of the Legal and Business Tensions in Information Privacy." *Yale Journal of Law & Technology* 4.

The TJX Companies, Inc. (TJX) Letter from TJX's President and CEO. 29 February 2008. <http://www.tjx.com/index.html> (15 March 2008).

Thatcher, Margaret. 1987. Interview for *Woman's Own* [excerpt]. <http://www.margaretthatcher.org/speeches/displaydocument.asp?docid=106689> (24 February 2008).

Thrift, Nigel and Shaun French. 2002. "The Automatic Production of Space." *Transactions, British Institute of Geographers* 27: 309-335.

Thrift, Nigel. 2004. "Cities Without Modernity, Cities With Magic." In *The Cybercities Reader*. Ed. Stephen Graham. London, UK and New York: Routledge.

Turban, Efraim and Jay E. Aronson. 2001. *Decision Support Systems and Intelligent Systems*. Upper Saddle River, NJ: Prentice Hall.

Urry, John. 2000. *Sociologies Beyond Societies: Mobilities for the Twenty-first Century.* London and New York: Routledge.

-------. 2006. Complexity. *Theory, Culture & Society* 23 (2-3): 111-117.

Vardoulakis, Dimitris. 2006. "The Return of Negation: The Doppelgänger in Freud's 'The Uncanny'." *SubStance* 35(2): 100-116.

w3.org. 2007. Enabling Smarter Privacy Tools for the Web. 20 November 2007. <http://www.w3.org/P3P/> (14 February 2008).

Wagner, R. Polk. 2005. "On Software Regulation." *Southern California Law Review* 78: 457-520.

Wall, David S. 2003. "Policing Elvis: Intellectual Property Rights, Legal Action and the Shaping of Post-mortem Celebrity Culture as Contested Space." *Entertainment Law* 2 (3): 35-69

Ward, Mark. 2007. How Firms and Fraudsters Deal in Data. 21 November 2007. <http://news.bbc.co.uk/2/hi/technology/7105212.stm> (10 January 2008).

Warner, Jeremy. 2005. "The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps." *University of Ottawa Law & Technology Journal* 2: 75-104.

Warren, Samuel D. and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 5 (5).

Webber, Andrew J. 1996. *The Doppelganger: Double Visions in German Literature.* Oxford, UK: Clarendon Press.

Weiser, Mark. [1991] 1999. "The Computer for the 21st Century." *Mobile Computing and Communications Review* 3 (3): 3-9.

Westin, Alan. 1967. *Privacy and Freedom.* New York: Atheneum.

Williams, Raymond. [1974] 1990. *Television: Technology and Cultural Form.* Ed. Ederyn Williams. London: Routledge.

Wright, S. and A. Steventon. 2006. "Intelligent Spaces: The Vision, the Opportunities, and the Barriers." In *Intelligent Spaces: The Application of Pervasive ICT.* Ed. Alan Steventon and Steve Wright. London: Springer.

Yeung, Albert and G. Brent Hall. 2007. *Spatial Database Systems.* Netherlands: Springerlink.

Živković, Milica. 2000. "The Double as the "Unseen" of Culture: Toward a Definition of Doppelganger." *Facta Universitatis* 2 (7): 121-128.

Zwick, Detlev and Nikhilesh Dholakia. 2004. "Whose Identity is it Anyway? Consumer Representation in the Age of Database Marketing." *Journal of Macromarketing,* 24 (1): 1-42.

Canadian Statutes

Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5 [PIPEDA] <http://laws.justice.gc.ca/en/ShowDoc/cs/P-8.6///en?page=1>.

***Privacy Act*, R.S.C. 1985, c. P-21 <http://laws.justice.gc.ca/en/showdoc/cs/P-21///en?page=1>.**