

4 of 4 DOCUMENTS

Copyright (c) 1998 The Board of Trustees of Leland Stanford Junior University
Stanford Law Review

50 Stan. L. Rev. 1193

LENGTH: 39396 words

ARTICLE: Information Privacy in Cyberspace Transactions

Jerry Kang *

* Acting Professor, University of California at Los Angeles ("UCLA") School of Law. kang@law.ucla.edu; <<http://www.law.ucla.edu>>
For helpful conversations and comments, I thank Rick Abel, Keith Aoki, Stephen Bainbridge, Paul Bergman, Stuart Biegel, Gary Blasi, Daniel Bussel, Evan Caminker, Ann Carlson, Margaret Chon, Richard Fallon, Catherine Fisk, Jody Freeman, Robert Heverly, Peter Huang, Kenneth Karst, Ken Klee, William Klein, Stan Kurzban, Mark Lemley, Larry Lessig, Gillian Lester, Gerald Lopez, David Post, Gary Rowe, Pamela Samuelson, Rick Sander, Gary Schwartz, Paul Schwartz, Seana Shiffrin, David Sklansky, Clyde Spillenger, Kirk Stark, Richard Steinberg, Eric Talley, Eugene Volokh, John Wiley, Stephen Yeazell, and Fred Yen. Special thanks go to my colleague Mitu Gulati. Preliminary thoughts were presented to the 1996 Conference of Asian Pacific American Law Faculty, at UCLA School of Law, the Junior Faculty Group at UCLA, and the UCLA School of Law Faculty Colloquium. I thank my research assistants, Philip Lee, Paul Ohm, Jean-Paul Saulnier, and especially John Padovan for expert assistance, which was funded by grants from the UCLA Academic Senate, the UCLA Asian American Studies Center, and the UCLA School of Law Dean's Fund. As always, the staff of the Hugh & Hazel Darling Law Library at UCLA was enormously helpful. I worked on some of the government reports I critique; a full disclosure appears in note 19 *infra*. I dedicate this to my confidant, Sung Hui Kim.

TEXT:
[*1193]

Cyberspace is the rapidly growing network of computing and communication technologies that have profoundly altered our lives. We already carry out myriad social, economic, and political transactions through cyberspace, and, as the technology improves, so will their quality and quantity. But the very technology that enables these transactions also makes detailed, cumulative, invisible observation of our selves possible. The potential for wide-ranging surveillance of all our cyber-activities presents a serious threat to information privacy. To help readers grasp the nature of this threat, Professor Jerry Kang starts with a general primer on cyberspace privacy. He provides a clarifying structure of philosophical and technological terms, descriptions, and concepts that will help analyze any problem at the nexus of privacy and computing-communication technologies. In the second half of the article, he focuses sharply on the specific problem of personal data generated in cyberspace transactions. The private sector seeks to exploit this data commercially, primarily for database marketing, but many individuals resist. The dominant approach to solving this problem is to view personal information as a commodity that interested parties should contract for in the course of negotiating a cyberspace transaction. But this approach has so far failed to address a critical question: Which default rules should govern the flow of personal information when parties do not explicitly contract about privacy? On economic efficiency and human dignity [*1194] grounds, Professor Kang argues in favor of a default rule that allows only "functionally necessary" processing of personal information unless the parties expressly agree otherwise. The article concludes with a proposed statute, entitled the Cyberspace Privacy Act, which translates academic theory into legislative practice.

[*1195]

Introduction

Cyberspace is shorthand for the web of consumer electronics, computers, and communication networks that interconnects the world. n1 Coursing through this web is information, which makes useful our telephones, radios, televisions, pagers, faxes, satellite dishes, and computer networks. The revolution in our communications infrastructure – in particular, the explosive growth n2 of the Internet n3 – has fundamentally transformed how we create, acquire, disseminate, and use

information.

The benefits are striking. Now, digitized libraries make available vast resources, regardless of distance. n4 Telemedicine allows remote experts to advise local caregivers. n5 Shopping and entertainment can be accessed im- [*1196] mediately through virtual malls and auditoriums. n6 Individuals now debate the day's burning issues in electronic fora, oblivious to geographical separation. n7

Unfortunately, cyberspace also raises new concerns. Consider, for example, the much-publicized conflicts concerning cyberspace copyright n8 and pornography. n9 The buzz around these issues is not surprising; intellectual property and freedom of expression are critical to our economics and politics. But cyberspace presses upon us a third issue, the significance of which is less obvious. That issue is privacy, what Justice Louis Brandeis once called "the most comprehensive of rights and the right most valued by civilized men." n10

The public is already apprehensive about privacy. For example, a 1996 study conducted by Equifax, a leading credit bureau, and Alan Westin, a privacy scholar, found that 89% of those polled in the United States were either [*1197] very or somewhat concerned about privacy. n11 Some of the most extensive surveys of Internet users indicate that cyberspace will exacerbate that anxiety. n12 This growing concern recognizes, if vaguely, that, as our communica- [*1198] tions infrastructure grows more powerful and user-friendly, we increasingly speak, listen, and act through cyberspace. And such activity generates records, dutifully recorded, sorted, saved, and exchanged by computers. n13

To focus that vague concern, imagine the following two visits to a mall, one in real space, the other in cyberspace. In real space, you drive to a mall, walk up and down its corridors, peer into numerous shops, and stroll through corridors of inviting stores. Along the way, you buy an ice cream cone with cash. You walk into a bookstore and flip through a few magazines. Finally, you stop at a clothing store and buy a friend a silk scarf with a credit card. In this narrative, numerous persons interact with you and collect information along the way. For instance, while walking through the mall, fellow visitors visually collect information about you, if for no other reason than to avoid bumping into you. But such information is general - e.g., it does not pinpoint the geographical location and time of the sighting - is not in a format that can be processed by a computer, is not indexed to your name or another unique identifier, and is impermanent, residing in short-term human memory. You remain a barely noticed stranger. One important exception exists: The scarf purchase generates data that are detailed, computer-processable, indexed by name, and potentially permanent.

By contrast, in cyberspace, the exception becomes the norm: Every interaction is like the credit card purchase. The best way to grasp this point is to take seriously, if only for a moment, the metaphor that cyberspace is an actual place, a computer-constructed world, a virtual reality. In this alternate universe, you are invisibly stamped with a bar code as soon as you venture outside your home. There are entities called "road providers," n14 who supply the streets and ground you walk on, who track precisely where, when, and how fast you traverse the lands, in order to charge you for your wear on the infrastructure. As soon as you enter the cyber-mall's domain, the mall begins to track you through invisible scanners focused on your bar code. It automatically records which stores you visit, which windows you browse, in which order, and for how long. The specific stores collect even more detailed data when you enter their domain. For example, the cyber-bookstore notes which magazines you skimmed, recording which pages you have seen [*1199] and for how long, and notes the pattern, if any, of your browsing. It notes that you picked up briefly a health magazine featuring an article on St. John's Wort, read for seven minutes a newsweekly detailing a politician's sex scandal, and flipped ever-so-quickly through a tabloid claiming that Elvis lives. Of course, whenever any item is actually purchased, the store, as well as the credit, debit, or virtual cash company that provides payment through cyberspace, takes careful notes of what you bought - in this case, a silk scarf, red, expensive. n15

All these data generated in cyberspace are detailed, computer-processable, indexed to the individual, and permanent. While the mall example does not concern data that appear especially sensitive, the same extensive data collection takes place as we travel through other cyberspace domains - for instance: to research health issues and politics; to communicate to individuals, private institutions, and the state; and to pay our bills and manage our finances. Moreover, the data collected in these various domains can be aggregated to produce telling profiles of who we are, as revealed by what we do and say. The very technology that makes cyberspace possible also makes detailed, cumulative, invisible observation of our selves possible. One need only sift through the click-streams generated by our cyber-activity. The information we generate as a by-product of this activity is quite valuable. The private sector seeks to exploit it commercially, but individuals resist. Both sides lay powerful, clashing claims to this data generated in cyberspace. How we resolve this conflict warrants careful discussion.

A conversation about privacy, of course, has been ongoing for a long time. In American law alone, it is over a century old. n16 And, for the past three decades, many have warned about the privacy dangers posed specifically by the computer. n17 That privacy conversation must now be broadened to consider the impact of the entire communications infrastructure. Not surprisingly, academics have started to address these new issues. n18 More sur- [*1200] prisingly, government has also tried to stay ahead of the curve. n19 The goal of this article is to push the conversation forward by uniting the thinking of both worlds. Methodologically eclectic, it draws where useful from philosophy, network engineering, and economics to supplement more traditional doctrinal analysis and legislative drafting.

Structurally, the article divides in half. The first half is a general primer on cyberspace privacy. It begins, in Part I, by clearing the conceptual and linguistic underbrush. Specifically, I identify equivocations latent in the term "privacy," present a definition widely accepted in the policy literature, and explore the conceptual consequences of that definition. Part II then examines what is technologically different in cyberspace and how information privacy will be threatened by new technologies unfettered by old laws. My purpose here is foundational – to build a clear and technically correct structure of terms, descriptions, and concepts. This half should facilitate the analysis of any problem at the nexus of privacy and computing–communication technologies. It is regrettably, but necessarily, long and detailed.

[*1201] Having built this foundation, the article changes gears in the second half. In aim, it moves from descriptive mapping to normative problem–solving. In scope, it narrows its focus to just one of the many privacy issues that the primer unearths, namely the problem of personal data specifically generated in the course of executing a cyberspace transaction. Specifically, in Part III, I describe the dominant normative approach to the problem, championed by various commentators and suggested in recent federal policy proposals. This approach urges the construction of a market for personal information, which is viewed no differently than other commodities that the market is supposed to price correctly and allocate efficiently. The marketplace approach has many attractions, but it is, as currently conceptualized, seriously incomplete. It fails to address which default rules should govern the flow of personal information when parties do not explicitly contract about privacy. On efficiency and nonefficiency grounds, I argue in favor of a default rule that allows only "functionally necessary" processing of personal information unless the parties expressly agree otherwise. Finally, in Part IV, I translate academic argument into pragmatic policy. The end result is a proposed Cyberspace Privacy Act, which would govern the processing of personal information collected in the course of executing cyberspace transactions in the United States.

An important limit to my project is that it does not examine how privacy may be violated by the state in the course of, for example, doling out public benefits, collecting taxes, or deterring crime in and through cyberspace – although these, too, present critical social issues. Instead, the spotlight is on the private sector and how it processes personal information in the little–regulated marketplace of ideas, information, and goods that is cyberspace. Equally important issues regarding governmental invasion of privacy exist, but I table those for now, partly because they have already received substantial attention. n20 In contrast, private actors' impact on privacy has undergone less exacting scrutiny, which is unwarranted; the private sector has come to rival government in the use of personal information. n21 With this proviso, I [*1202] begin by examining the constituent components of the term "cyberspace privacy." I start with privacy.

I. Privacy: A Philosophical Clarification

It is cliché to note that the threshold obstacle to clear thinking about privacy is the term itself. Privacy is a chameleon that shifts meaning depending on context. n22

A. Three Clusters: Space, Decision, and Information

The term "privacy" conveys numerous ideas that can be clustered into three groupings. The first cluster concerns physical space – in particular, the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals. This spatial privacy is the sort invoked by sociologists who discuss private versus public territories and territorial overcrowding. n23 It is this sense of privacy that informs the Fourth Amendment search–and–seizure concept of curtilage. n24 This is also the sense of privacy employed when one complains about a car alarm or a telemarketing call disturbing one's privacy.

The second cluster views privacy as principally concerned with choice, an individual's ability to make certain significant decisions without interference. This decisional privacy is the sort discussed famously in *Roe v. Wade*. [*1203] n25 This conception of privacy is less concerned with the maintenance of spatial boundaries and more concerned with a person's freedom to make self–defining choices without state interference. n26 Of the three privacy clusters I will mention, this one has incited the most contentious constitutional and political battles.

Finally, the third cluster of privacy concerns the flow of personal information. More precisely, information privacy concerns an individual's control over the processing – i.e., the acquisition, disclosure, and use – of personal information. In this third cluster, the paradigmatic privacy violation does not occur, for instance, when the state places an undue burden on some significant decision. Rather, this strand of privacy is invaded when, for example, someone obtains sensitive medical data by rifling through confidential files without permission.

I use the term "cluster" to connote that these three types are not sharply separate. They are functionally interconnected and often simultaneously implicated by the same event or practice. For instance, spatial privacy often promotes information privacy: When one is shielded from external stimuli, such that signals – say, the sound wave of a barking dog – cannot flow to the individual, one is often simultaneously shielded from observation, such that signals cannot flow outward from the individual. n27 Being so shielded from observation means that personal information cannot be collected, which bolsters an individual's privacy. n28 As another example, consider how information privacy – e.g., keeping the fact of pregnancy to oneself – can create the breathing space away from familial or societal censure necessary for decisional privacy – e.g., to choose whether to have an abortion. n29 Or, in reverse, [*1204] consider how decisional privacy shields an individual from disclosing to the state her justifications for exercising some choice, thereby fortifying her information privacy. Finally, note how receiving unwanted solicitations through mail, telephone, or e-mail can simultaneously implicate two distinct privacy clusters. The junk mail, phone call, or message invades my space, spamming my physical, voice, and electronic mailboxes. n30 More importantly but less obviously, the initial targeting of that junk mail to me may have involved access to and analysis of personal information, namely my tastes, life events, and consumption history.

Indeed, a serious argument can be made that all three and additional privacy clusters can be integrated into a single, abstract cluster grounded in some moral value such as human dignity n31 or inviolate personality, n32 some sociopsychological process such as interpersonal boundary maintenance n33 or access to the self, n34 or some political theory such as antitotalitarianism. n35 But as intriguing as such grand unification projects may be, my focus lies elsewhere. From a practical point of view, the debate over reproductive freedom is usefully seen as a debate different from the one about personal information. n36 In keeping the clusters separate, I take no position on the ultimate success of a grand unification theory. n37 Instead, my point is simply to pare down concepts into usable components, flag equivocations in the term "privacy," and delimit more precisely the scope of my inquiry. To be explicit, [*1205] my inquiry focuses on the third privacy cluster, information privacy. n38 Although this cluster may not be privileged in analytic priority or policy significance over the other two, it is precisely this sort of privacy that cyberspace most threatens.

B. Focus: Information Privacy

Information privacy is "an individual's claim to control the terms under which personal information – information identifiable to the individual – is acquired, disclosed, and used." n39 This definition comes from Principles for Providing and Using Personal Information ("IITF Principles"), issued by the Clinton administration's Information Infrastructure Task Force. n40 I adopt the IITF's definition because it is analytically useful, consistent with a broad swatch of academic and policy thinking, n41 and likely to be influential in gov- [*1206] ernmental, private sector, and academic discussion. n42 If history repeats itself, it will be the foundation for future federal privacy legislation. n43

1. Personal information.

Not surprisingly, the central component of this and nearly all definitions of information privacy is the term "personal information." n44 It is also the least self-explanatory. n45 For example, the IITF Principles define personal information as "information identifiable to the individual." n46 In other words, "personal" does not mean especially sensitive, private, or embarrassing. n47 [*1207] Rather, it describes a relationship between the information and a person, namely that the information – whether sensitive or trivial – is somehow identifiable to an individual.

But what does it mean for information to be "identifiable to an individual"? In my view, information can be identifiable to an individual in three ways: It can bear (1) an authorship relation to the individual, (2) a descriptive relation to the individual, or (3) an instrumental mapping relation to the individual. First, the individual could have purposefully created or prepared the information – typically to communicate that information to another party – such that an authorship relationship connects the individual to the information. This relationship explains why a telephone conversation, personal diary, love letter, or e-mail constitutes personal information. n48

Second, the information could describe the individual in some manner besides the above authorship relation. On the one hand, it could speak to some permanent or nonfleeting status of the individual, either biological or social. For example, it could describe the individual's biometric state, such as sex, height, weight, blood type, fingerprint, retina pattern, DNA,

or state of health. It could relate biographical facts, such as birth date, marital status, sexual orientation, immigration status, criminal history, or educational degrees. It could identify social connections, such as membership in religious and political organizations. On the other hand, descriptive information could record more discrete, transient actions taken by an individual. For example, it could chronicle that a particular individual visited a particular store at a particular time to purchase a particular item. Such information is routinely collected during undercover surveillance. Of course, in cyberspace, surveillance is not performed through traditional methods, such as a private investigator parked outside the target's home with thermos and binoculars. Instead, it is done through cyberspace itself, by collecting and sifting the data trail left by the individual's cyber-activity. n49

Third, information not in the above two categories may still be personal if it is instrumentally mapped to the individual for institutional identification, [*1208] secured access, or provision of some service or good. Usually, such information bears no prior relation to the individual. The best example is the Social Security number. In no way does the individual create or author the number. Nor does it describe the individual's state-of-being or actions, except that it is mapped to the individual by the federal government for recordkeeping purposes. This category of personal information includes confidential n50 pieces of information that act as keys to secured functions or processes, such as passwords to login to a network and to use automatic teller machines.

These three categories are not mutually exclusive. For instance, an e-mail that describes a specific individual is personal in at least two different senses. It is personal vis-a-vis the sender of the e-mail in an authorship relation; it is personal vis-a-vis the individual mentioned in a descriptive relation. Also, certain types of information that are personal in an instrumental mapping sense may be personal in a descriptive sense. Consider the common practice of using the mother's maiden name as a password for remote access to one's bank account. Viewed solely as a key to secured processes, it is an instrumentally mapped piece of personal information; viewed as disclosing familial relationships, it is a descriptive piece of personal information. Despite some overlap, these three categories clarify the different ways in which a datum might be "personal," differ enough so as to be conceptually useful, and span the space of personal information.

2. Nonpersonal information.

If information bears no linkage to an individual, then it is not personal information and, according to the definition of privacy, lacks privacy significance. The link may be missing in three ways. First, the information simply may not be about an individual human being. For instance, the datum "[pi] is [*1209] 3.14 to three significant digits" is not linked to any individual via an authorship, description, or instrumental mapping relation. Therefore, it is not personal information, which means it poses no privacy concerns.

Second, although about an individual, the information may not be identifiable to that specific individual because it has been anonymized. Consider, for example, an anonymous poll conducted by phone, in which responses are not linked to the telephone number, and the individual's identity is never ascertained. Here, by hypothesis, the data cannot be traced back to the specific individual from whom they were collected. Thus, although the data are about the views of human beings, they are not personal information and seemingly pose no privacy threat.

But we must recognize that anonymity comes in shades. Although no specific individual is identified facially, the individual may be identifiable in context or with additional research. n51 A prime example of such superficial anonymity is the interviewee - typically victim, witness, or whistle-blower - who is ensured anonymity by law enforcement or the media, but is nevertheless recognized under the totality of the circumstances. n52

A more subtle qualification also deserves mention. Imagine that a psychiatrist publishes verbatim counseling notes in a best-selling book, but in a way that the specific identity of the patient cannot be determined. If the patient protests at having her story chronicled in agonizing detail to the public, could the good doctor respond that because the information is not identifiable to the specific patient, even with additional research, it is not "personal information." And, because it is not personal information, the patient lacks any privacy claim? To my mind, this reasoning fails to account for the residual privacy interest that exists, notwithstanding the anonymity. Recall that privacy involves the control of the flow of personal information in all stages of processing - acquisition, disclosure, and use. Simply because the information is anonymized at the disclosure and use stages, and thus not personal in one sense, does not mean that it was not personal information when originally acquired from the individual. This refutes the doctor's claim that no "personal information" is at stake. In other words, a genuine privacy claim is in play. n53

[*1210] Third, although about individuals and not anonymized, the information is directly identifiable to a group and only indirectly identifiable to the individuals constituting that group. Under one interpretation of the privacy definition,

because the information is directly about the group and not the individuals that constitute the group, the data are not personal and stand outside privacy's realm. But this seems formalistic. A more functional approach would recognize that groups, even those recognized as legal persons, function only through the actions of the human individuals who are its members. Accordingly, information concerning a group concerns also those individuals that constitute the group. What we ultimately label as "personal" should thus depend on context, such as the size of the group and the degree of focus the information places on some subset of that group.

With this nuanced, functional understanding, we can better answer the perplexing question whether, for example, a corporation has privacy interests. A corporation qua corporation does not. Only the individuals that make up the corporation do. This does not mean that the corporation must lack standing to argue the privacy interests of its constituent individual members. It does mean, however, that the foundation of any such group privacy claim lies originally in the interests of individual human beings. n54

In practice, then, the answer to group privacy questions turns on context. On the one extreme, we can have information such as "IBM's stock is at thirty points today." In some ways, this information is identifiable to all those individuals affiliated with IBM, as directors, officers, and shareholders, but the link is so diffuse that I am comfortable classifying this datum as not personal information. At the other extreme, we can have information that a closely held corporation with one stockholder and two officers evaded taxes. This information is tightly enough linked to few enough people that it should be considered personal information. n55

[*1211] Rest assured that this nuanced view of group privacy will not leave corporate entities – which, like individuals, surely have their secrets n56 – unable to control the flow of information about themselves. Even if such data cannot be controlled under the rubric of privacy, they can be managed through alternate legal categories, such as contract, tort, and intellectual property. n57 Indeed, a potent array of unfair competition, trade secret, patent, trademark, and copyright law, in addition to confidentiality agreements, n58 support an institution's ability to control various types of information identifiable to itself. n59 In addition, collective entities often have the wherewithal to employ self-help security n60 measures so that information in their control flows only in ways they choose.

[*1212]

C. Privacy's Values

1. Values.

Now that we know what information privacy is, we should probe what purpose it serves. n61

Avoiding embarrassment. In any given culture, disclosures of certain behaviors, actions, or fates will embarrass the individual – even when the behavior, action, or fate is neither blameworthy nor stigmatized. Take urination for example. There is nothing wrong with urination; all humans do it. The fact that someone urinates is not going to be used against her. However, a visual disclosure of that behavior – for instance, being caught on videotape through a hidden camera – would cause intense embarrassment for most Americans. Another example is minor hemorrhoids. Assume that this fact will not be used against the person in any way. The individual will not pay more for health insurance, will not drop in social standing, and will not lose her job or friends. Nevertheless, the broad disclosure of this fact would embarrass many, perhaps most, people.

That these examples are culturally contingent makes them no less real. n62 In other words, the fact that different cultures may react differently to such disclosures does not deny that, for each culture, there are some zones of behavior, actions, or fates the disclosure of which – in and of itself – will cause discomfort or embarrassment. n63 One value of information privacy, then, is to avoid the simple pain of embarrassment.

Constructing intimacy. An individual's capacity to disclose personal information selectively also supports her ability to modulate intimacy. Charles Fried has argued this case most prominently. n64 By virtue of information privacy, one can selectively regulate the outflow of personal information to others. By reducing this flow to a trickle, one can construct "aloofness, removal, and reserve," n65 and maintain substantial social distance. Conversely, [*1213] one can release a more telling flow of personal information, n66 which invites and affirms intimacy. n67

According to Fried, information privacy is necessary to create social relationships that go beyond the basic respect due all human beings. n68 Something in addition to basic human respect must exist between two individuals to transform their relationship into one of trust, friendship, or love. That additional something is intimacy, which is partly created by the

release of secrets – the selective disclosure of personal information. n69 Without information privacy, we would be less able to disclose on a case-by-case basis the nonpublic facets of our personality. Thus, we would lack the "moral capital" n70 needed to construct intimacy. n71

I concur with Jeffrey Reiman's critique of Fried that intimacy is more related to the sharing of experiences than the sharing of secrets. n72 This does not mean that information privacy has nothing to do with modulating intimate relationships. I believe that intimacy, at least for adults in current American culture, involves the display of certain behaviors unseen in public areas, such as playfulness, childlikeness, and certain types of physical touching – which take root and flower best in an information preserve, away from the harsh light of publicity. n73 If we were under observation, we would not be able to display caring to other individuals as freely, spontaneously, or completely as we might otherwise. n74 This, in turn, would hinder the construction of deep social relationships.

[*1214] Averting misuse. Yet another value of privacy is that it protects against improper uses of personal information. Personal information can be misused in two ways. First, it can derail an otherwise fair process that distributes benefits and burdens. Many social goods – such as jobs, offices, remuneration, and respect – as well as social bads – such as unfriendliness, disrespect, and imprisonment – are granted or denied on the basis of data about ourselves. If these social goods and bads are allocated based on personal data of poor quality, unfairness may result: Garbage in, garbage out. n75 Further, high quality information in one context may be low quality information in another because, as Kenneth Karst explains, "the evaluator and the recipient of his statement may not share the same standards for reducing a complex set of facts to evaluative inferences or even the same language." n76 Worse, such decisions may be difficult to discover and correct, n77 especially when they are generated through automated processes. Computers, with their air of objectivity and infallibility, resist dispute. n78 One way to check against such information misuse is to give the individual greater control over the flow of personal information. An individual with such control will take preventative measures, [*1215] for instance, by keeping irrelevant personal data away from the decisionmaker. n79

Second, information can be misused by making us vulnerable to unlawful acts and ungenerous practices. After all, personal information is what the spying business calls "intelligence," and such "intelligence" helps shift the balance of power n80 in favor of the party who wields it. n81 To take a simple example, knowledge of our home phone number and address makes us more vulnerable to harassers n82 and stalkers. n83 Personal information can also make us vulnerable, for instance, to identity theft. n84 Besides outright illegal acts, another's control of our personal information can make us susceptible to a whole range of ungenerous practices. It could subject us to influence that crosses the line between persuasion and undue influence. Sophisticated advertisers, for example, do not merely track consumer demand; they manufacture it outright. n85 Detailed knowledge of who we are and what we consume makes the job of preference fabrication that much easier. n86 More disturbingly, personal information can be misused by making us vulnerable to prejudice or unwarranted disesteem. An example is the information that one is gay, which could be evidenced by accessing certain Internet discussion groups or making certain cyberspace purchases. n87 For those not generally "out," the inability to control this information creates tremendous social and psychological vulnerability.

Individual vulnerability has social consequences. It chills individuals from engaging in unpopular or out-of-the-mainstream behavior. While uniform obedience to criminal and tort laws may deserve praise, not criticism, excessive inhibition – not only of illegal activity but also of legal, but unpopular, activity n88 – can corrode private experimentation, deliberation, and reflection. n89 The end result may be bland, unoriginal thinking n90 or excessive [*1217] conformity to unwarranted social norms. n91 Worse, the self-repression of activity and communication could undermine the self-critical capacities of a polity. n92 This is why totalitarian regimes have maligned a desire for privacy as deviant, in part to sap an individual's ability to question the status quo and to experiment with alternate conceptions of the good life. n93

2. Countervalues.

It would be one-sided to discuss only the values supporting information privacy when prominent countervalues – values against individual control over personal information – also exist.

Commerce. By requiring the individual's consent before personal data are processed, privacy applies friction to the flow of information. This friction, the argument goes, hurts commerce; better information leads to better markets. When this argument is made, two stories are often told – one about junk mail, the other about consumer credit. The junk mail story starts by explaining that junk mail is only "junk" because it was sent to the wrong person. If the direct marketing industry had better intelligence about personal interests and preferences – for example, by being able to examine an individ- [*1218] ual's history of consumption – people would receive less "junk." Because information privacy makes this more difficult, it

increases the search costs of matching interested buyers with interested sellers. In short, more privacy means more junk. The consumer credit story starts by noting that a freer flow of personal information can decrease the costs of consumer credit by helping creditors avoid bad credit risks. Additional personal information allows greater discrimination among individuals according to whatever characteristic is relevant to a particular transaction. n94 This, in turn, decreases the cost of such transactions either generally, or, at the least, for those individuals who possess a favorable set of characteristics. n95

The commerce argument, as thus stated, presumes that privacy necessarily entails information blockage. But this is not so. If individuals will truly benefit by releasing their personal data, e.g., by getting less junk or cheaper credit, they will rationally choose to do so. n96 Information privacy does not mandate informational quarantine; it merely requires that the individual exercise control within reasonable constraints over whether, and what type of, quarantine should exist. Accordingly, these arguments do not demonstrate that the individual should be deprived of information privacy. At most, they suggest that individuals should be open to information processing in exchange for commercial benefit and that society should make such exchanges feasible. n97

Truthfulness. Information privacy allows one to have thoughts, beliefs, conditions, and behaviors without the knowledge of others, thereby making it easier to have public personae distinct from private ones. This differentiation between public and private visages need not be used for good, such as self-determination and deliberative politics. Instead, the argument goes, it will be used to deceive and defraud. Individuals will not only keep poor quality information away from decisionmakers, they will also conceal high quality, but legitimately detrimental, information. The cover of privacy might encourage individuals not only to engage in activity unjustifiably stigmatized but also justifiably [*1219] stigmatized. Worse, they may be hypocrites, publicly espousing norms they privately abandon. n98 The parade-of-horribles conjures easily: the unrehabilitated child molester volunteering for day care; the domestically violent tyrant passing as winsome celebrity; the sexually promiscuous person, infected with herpes, claiming to be disease free; the reckless driver swearing falsely to be accident free. Perhaps Richard Posner was right to recast invasions of privacy as self-defense against deception. n99

It would be facile to deny that information privacy can cloak our darker sides and aid misrepresentation. Equally facile, however, is the inference that information privacy is thus inexorably the handmaiden of deception. Privacy is not valuable only to those with something discreditable to hide. Individuals do not always seek to conceal or control personal information to exploit others in some acquisitive, tortious, or immoral way. n100 Put in other terms, secrecy – the intentional concealment of personal information – does not always amount to lying. n101 The hallowed example is the secret ballot. n102

Moreover, it is not inherently wrong for individuals to have differing private and public masks. n103 Consider how differently we act, and rightly so, between work and home. Only an unsophisticated psychology assumes one true, essential personality, with all other personae spurned as deceitful masks. In fact, all our masks, all our roles, constitute integral facets of our personalities, none of which is necessarily privileged, true, or authentic. n104 This is not to say that no core personality exists. But this core personality is a weighted composite of the multiple personalities we experience and cultivate. n105 The ability to maintain divergent public and private personae creates the elbowroom necessary to resist social and political homogeneity. n106

In sum, information privacy does not necessarily promote deception and fraud. It can do so only if both the nature of the relationship between the individual and the information user, and the ethical or legal duties of disclosure inherent to that relationship, command an openness that information privacy prevents. What is important is that in most cyberspace transactions, which I describe below, far more information is collected than any self-defense "need to know" principle could justify.

II. Cyberspace: A Technical Description

A. Cyberspace Introduced: A Brave New World

The neologism "cyberspace" is shorthand for the emerging Global Information Infrastructure ("GII"). The GI, like all information infrastructures, moves information from sender to receiver through some medium. In cyberspace, information typically moves through a hybrid of wireline n107 and wireless pathways. n108 For example, cable television signals are delivered to [*1221] the local cable television company through wireless satellite feeds, but are then carried to the home via a hybrid wireline of optical fiber and coaxial cable. From the user's perspective, the exact path the information takes from place to place is irrelevant. What is important is that the information transfers with speed and security. n109

Once information is transported, it is processed to provide some communicative functionality. For example, information transferred through our public, switched telephone network is processed to provide oral communications, low-resolution printouts (e.g., facsimiles), and low bandwidth links to computer networks such as bulletin board services (or BBSes), proprietary on-line services, n110 and the Internet. n111 Information transferred through wireless broadcast systems, such as direct-broadcast satellite and wireless cable, may be processed into video signals that provide traditional broadcast television-like content.

Cyberspace transfers, processes, and stores information faster, cheaper, and better than any information infrastructure we have had before. Faster transfer rates mean that video that once took an hour to download through a standard Internet connection now takes minutes. n112 Improved processing [*1222] means that users now can search efficiently through the vast cyber-sea of information through easily navigable interfaces. Improved storage means that cost concerns no longer loom large in forcing the reuse of storage media, such as hard drives. n113

Converging improvements in information transfer, processing, and storage will soon produce a communications system that combines the high-bandwidth of our cable networks, the bidirectionality n114 and addressability n115 of our public, switched telephone networks, and the point-and-click computer interface of the World Wide Web (the "Web"). n116 Accordingly, cyberspace of the near-future will likely look like an applet-enabled n117 Web, with data transfer rates fast enough to exchange not only text, but also real-time video and iconic or avatar interfaces far friendlier than today's. Local exchange carriers ("LECs"), n118 cable companies, n119 and their joint ventures are rebuilding their networks to provide such interactive, high-bandwidth, communication channels. n120 The technological advances in computer processing [*1223] and communications that are making this future possible are announced almost daily.

Putting the technological bells and whistles aside, such a network is or will soon be the epitome of convenience. The networked personal computer will become the one-stop information appliance for all types of transactions n121 that now take place in the physical world. These transactions will include the serious, such as news retrieval, research, education, banking, mailing, voting, tax filings, and telemedicine. They will also include the playful, such as shopping, games, movies, music, and socializing. Already, on the current information infrastructure, increasing numbers of people are executing such transactions. As the infrastructure upgrades, n122 and technological literacy explodes, more individuals will employ the new communications technologies to perform more transactions in cyberspace.

B. Cyberspace's Impact: A Mapping of Information Flows

From a privacy perspective, the crucial characteristic of cyber-activity is the rich flow of personal information it triggers. The schematic below represents an elementary electronic commerce transaction.

[SEE GRAPH IN ORIGINAL] [*1224] From home, an individual logs into her Internet Service Provider ("ISP") n123 through her computer and modem. She then launches her Web browser. She queries a search engine n124 for the name of a particular software application. After browsing through various merchant home pages, she finds an attractive offer. She selects the specific software package, pays for it by providing a credit card number, and downloads the program and related documentation. This ordinary transaction triggers myriad personal data flows.

1. Transacting parties.

First consider the principals to this economic transaction: the individual and the merchant. These transacting parties drive the transaction by exchanging a valuable good, i.e., the software program, for consideration, i.e., money. As a result of this transaction, the merchant has access to all the data that appear on a typical credit card receipt and shipping order. n125 If the merchant requests it, and the individual volunteers it, she may also have the individual's e-mail and physical addresses. n126 Even if such information is not volunteered, the merchant may collect it surreptitiously.

Technical map. When the individual browses a Web page, her computer - the client - provides various fields of information to the merchant's computer - the server. Roughly, these fields reveal some aspect of the client's (1) identity, (2) computer configuration, and (3) browsing activity.

First, the client must provide its own Internet Protocol ("IP") address to any server it contacts. n127 Every computer connected to the Internet is - [*1225] signed such an address, either temporarily or permanently. The Internet is a packet-switched n128 network of networks; information is broken down into packets, addressed, and fired off through the network to find its ultimate destination. In order for two computers on the Internet to communicate, each must know the other's IP address. n129 Since an IP address is hard to remember - my host computer's IP address is 149.142.28.67 - it is mapped to a more memorable domain name - my host computer's domain name is "kang.law.ucla.edu" n130 - pursuant

to the Domain Name System ("DNS"). n131 By convention, a server logs the IP address of each client that browses its site. From the IP address, a server can determine the domain name, if any, by performing a reverse look-up through the DNS. n132 Next, from the right portion of the domain name – in my case, the two right-most portions – the server can retrieve the name, physical location (e.g., country, state, and zip code), and contact persons of the organization that originally registered that name with the DNS. n133 In my case, the server can discover that I am affiliated with UCLA, which is located in Los Angeles, California. n134

[*1226] The identity information described so far pertains specifically to the client host computer, and not necessarily to the human individual using the computer. While it is true that in my case, my host computer has a domain name with my true last name "kang," this does not have to be the case. If the computer's domain name were "nomad.law.ucla.edu," then the server would have an IP address, the just mentioned domain name, and information about UCLA, but not any part of the individual's specific identity. There are two other ways, however, that the server may be able to access such information. If the individual had to authenticate herself, i.e., by typing in a unique user identification and password, to enter a restricted Web site, the server will be able to identify the specific individual assigned to that user identification. n135 In addition, if the client is configured in a particular manner – which is now uncommon since it is a security threat – then the server may be able to request the individual's local network login name, which is often some portion of the individual's last name. n136

The client also discloses to the server which human languages it prefers and to what degree it prefers them. n137 Since so much of the Web is in English, this datum is currently not so telling. But soon the Web will become more multilingual, and more users will set their language-preference options accordingly. This bit of information reveals the user's language abilities and, depending on the language, allows the server to make an intelligent guess about the user's ethnicity. n138

Second, in addition to the identity information discussed above, the Internet client will disclose some basic information about its computer configuration: the browser (e.g., Netscape Navigator or Microsoft Internet Explorer), the operating system (e.g., Mac OS, Windows 3.1, or Windows 95), and the hardware platform (e.g., IBM PC-compatible or Macintosh). n139

Third, the client will reveal something about its browsing activity. Each client visit to a server is typically logged. In addition to the identity information just described, this log includes: the time and date of visit; the Uni- [*1227] form Resource Locator ("URL") of the requested resource; n140 the byte length; and the URL of the resource from which the request was made (the "Referer"). n141 It bears mention that if I click on a link returned to me by a search engine, the server that I go to – by examining the Referer variable – can determine not only which search engine I used, but also which keywords I used in my query. n142 Finally, a server can track the "clicktrail" of a client – which means it can record which pages a client views – by order, time, and duration. Clicktrails can be maintained in one of two ways. The server can try to match the IP addresses and other identity information in its log to their time-stamps. Or, more easily, the server can set a "cookie."

A cookie is a piece of information sent by the server to the client to store for some time. Its purpose is to store information about the client's state, so as to personalize the browsing experience. For example, various Web servers provide movie listings by zip code. Because it is inefficient to require the user to reenter her zip code at each visit, the server saves the zip code and other "state information" on the client's hard drive in the form of a cookie. Thereafter, by accessing the cookie, the server can automatically present local movie features without querying the user for her location. Many personalized news services operate this way. One's preferences – for example, sports scores in Chicago or the weather in Boston – can be saved in a cookie. n143

Recently, there has been great public anxiety that cookies can be freely accessed by all Web servers we contact, thereby disclosing details about our browsing history. This fear is somewhat overblown: A client does not serve up cookies simply to anyone who asks. In other words, not all servers have access to all cookies. Each cookie, when initially set, circumscribes the [*1228] range of servers to whom the cookie may be subsequently given. The default range is the domain name of the server that initially set the cookie itself. n144 So, if the server hollywood.movienews.com set a cookie identifying my zip code as 90210 and did not specify a domain name range in the cookie, then, by default, the cookie would be presented only to hollywood.movienews.com in the future. While it is true that hollywood.movienews.com could have set the domain range to a larger set of servers, by setting the domain name range to the tail portion of its name, i.e., movienews.com, n145 it could not have set the range to an entirely different domain name, say, blockbuster.com. n146 Reciprocally, the client will only disclose a cookie to a server if the domain name range for the cookie "tail-matches" the server's domain name. In other words, a cookie with the domain name range movienews.com will not be disclosed to any server that has

the tail of blockbuster.com. As a result, cookies can usually be read only by those entities that wrote the cookie in the first place. n147

That said, there is nothing to keep companies like movienews.com and blockbuster.com from sharing with each other the browsing history of a given individual recorded through their respective cookies. In effect, this is what is done by various Internet advertising companies that target advertisement banners to individuals based on their browsing profile. n148 These advertising companies establish relationships with numerous Web servers. Whenever a client browses one of these Web pages, the client is fed an in-line image that invisibly connects it to the advertising company's server without the individual user's explicit knowledge or command. Once connected, the ad- [*1229] vertiser retrieves the identity information described above. On the one hand, if the client's IP address or domain name has not been seen before, the advertiser creates a unique identification number and saves it in a cookie on the client's hard drive. On the other hand, if the IP address/domain name has been seen already, then the advertiser accesses the previously set cookie, which contains a unique identification number, and updates the extant database record indexed by that number with the browsing activity of the client. Based on this database of browsing activity collected from all affiliated Web sites, the advertiser delivers a targeted ad banner. These transactions occur within a fraction of a second. n149

To summarize, a client's browsing behavior at a particular site can be tracked with detail. Through, for instance, the use of cookies, this tracking can continue over multiple visits, over an indefinite period of time, with all browsing information compiled into a database. This does not mean, however, that any other site has automatic access to this information - with the following critical exception: Sites may be linked together through a data sharing relationship, the most prominent of which is affiliation with a common advertiser.

These three types of disclosures - identity, computer configuration, and browsing activity - are not software bugs or security loopholes that will be corrected momentarily. n150 Rather, they are the standard, albeit unpopular, n151 elements of the Web browsing process. n152 Further, these personal informa- [*1230] tion flows can be leveraged to produce additional information, often cheaply and rapidly, through cyberspace. For example, an e-mail address or domain name may be reverse-indexed, using national computerized White Pages, to find, in many cases, the individual's name, telephone number, and physical address. Even unlisted information can sometimes be located through the use of national lookup databases. n153

Legal map. The collection of personal information in America by transacting parties is largely unregulated by law. Unlike certain European nations, n154 the United States has no omnibus privacy law covering the private sector's processing of personal information. Instead, American law features a patchwork of rules that regulate different types of personal information in different ways, depending on how it is acquired, by whom, and how it will be used. Since others have canvassed the positive law extensively, n155 my comments are summary.

To set the stage, federal constitutional law provides no protection of an individual's information privacy from invasion by the private sector - first, because of the state action doctrine, n156 and second, because it is unclear to what extent the Constitution actually protects information privacy. n157 The [*1231] state action doctrine similarly defangs state constitutional protections of information privacy where they exist. n158 Further, the common law tort of invasion of privacy has thus far provided no effective constraints on the sort of information flows depicted above. n159 Finally, general omnibus privacy stat- [*1232] utes, such as the federal Privacy Act and its state analogues, n160 fail because they apply only to government action. n161

There are, however, numerous statutes that govern specific sectors of personal information, such as consumer credit, n162 education, n163 cable programming, n164 electronic communications, n165 videotape rentals, n166 and motor vehicle records. n167 But it turns out that none of these statutes substantially constrains a transacting party from collecting the information identified above. More detailed analyses of specific statutes are provided where relevant.

2. Transaction facilitators.

Now let us focus on the category of players I call transaction facilitators, those who help execute the transaction but are not the principal drivers of the exchange. In this example, the telephone company, ISP, and credit card company are all transaction facilitators, which help to consummate the deal between the principal parties: the individual and the merchant. The two most common types of transaction facilitators are communications providers, which provide the channel through which the individual and merchant communicate, and payment providers, which arrange payment between the transacting parties. In this example, the telephone company and the ISP carry the communications, and the credit card company arranges for payment.

[*1233] Communications providers – Technical map. Communications providers, e.g., the telephone company and ISP, collect subscription data when an individual signs up for their services. n168 More specific to the software purchase, the communications providers have access to certain kinds of transactional data, such as routing information used to connect the individual and the merchant over the network. For example, the telephone company maintains, if temporarily, calling records identifying the originating number – the individual – destination number – the ISP – and, possibly, the time and length of the call. The ISP, on the other hand, will likely keep logs that identify the individual user, the remote computer contacted – in this case, the merchant's Web server – and the date and time of contact. Depending on the technological set-up, the ISP may also have transactional data of files uploaded or downloaded, and e-mail messages sent and received. n169

The above example assumes that the individual accessed cyberspace through a home connection, but individuals often jack into cyberspace through equipment provided by their employers. In this regard, employers thus may function as a sort of communication provider, by footing the bill for cyberspace access. In exchange for providing that access, employers often feel entitled to collect information about their employees' use of cyberspace. For example, many employers reserve and exercise the right to read their employees' e-mail. n170 Employers also use various software and network management tools to track employee cyber-activity, such as the Web sites visited and files downloaded. n171

Communications providers – Legal map. Communications providers, as all persons, must abide by the Electronic Communications Privacy Act of 1986 ("ECPA"). n172 The rough logic of the grossly complicated ECPA is to [*1234] break down electronic communications into two temporal periods, one during transmission and the other during storage. Title I governs the former; n173 Title II governs the latter. n174 During transmission, the ECPA proscribes the interception n175 of an electronic communication and the subsequent disclosure n176 and use n177 of its contents. But the handling of an electronic communication by a communications provider, in the ordinary course of business, does not constitute an "interception." n178 Similarly, the ECPA proscribes the "unauthorized access" n179 of an electronic communication while in storage in an electronic communication service facility. But again, access approved by the electronic communications provider is not deemed "unauthorized." n180

The ECPA also has specific confidentiality rules for communication providers that serve the general public. These providers cannot divulge the contents of the communications during transmission n181 or while in storage. n182 Although this may seem to bar communication providers from peddling personal information in the marketplace, such privacy protections are illusory. The above bar applies solely to the contents of communications, not to transactional records, which may be freely disclosed to anyone "other than a governmental entity." n183

[*1235] Unfortunately, the line is not bright between the contents of a communication and the transactional data about that communication. According to the ECPA, content "includes any information concerning the substance, purport, or meaning of that communication," n184 whereas transactional records are implicitly defined as "a record or other information pertaining to a subscriber to or customer of such [electronic communication] service." n185 The legislative history adds little light, except to make clear that "contents" do not include "the identity of the parties or the existence of the communication." n186 The upshot of this analysis is that the ECPA constrains a communication provider's exploitation of personal information in only limited ways. Although electronic communications providers to the public must keep the contents of communications confidential, they have almost n187 no such obligation regarding transactional records. n188

[*1236] Payment providers – Technical map. Another sort of transaction facilitator is the payment provider, which, in this example, is the credit card company. n189 As with the communication providers, the credit card company collects subscription data – in this case through a credit card application. For any specific purchase, the company would have the transactional data that appear on monthly billing statements: merchant name, city, and state; date of purchase; and amount of purchase.

Payment providers – Legal map. As to credit providers, an important federal law that may appear relevant is the Fair Credit Reporting Act ("FCRA"). n190 Unfortunately, the FCRA does not effectively constrain what these payment providers can do with the data that they have collected. The FCRA attempts to maintain the confidentiality and quality of "consumer reports," which are defined as any communication by a "consumer reporting agency" regarding "a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" n191 that is used for credit, insurance, employment, or other "legitimate business need." n192

The privacy rules of the FCRA are not likely to apply to payment providers because the data that they collect and subsequently disclose to others do not constitute "consumer reports" within the meaning of the Act. First, the payment

providers are not themselves consumer reporting agencies, because they do not regularly engage "in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties." n193 Second, the definition of "consumer report" explicitly excludes "any report containing information solely as to transactions or experiences between the consumer and the person making the report." n194 Finally, even if these definitional hurdles were cleared, courts have read the term "legitimate business [*1237] need" so broadly that the practice of exchanging credit reports could be justified by any number of reasons, including database marketing. n195

*** I offered the software purchase example to suggest a generic architecture with which to conceptualize transactions – an architecture that divides participants into transacting parties and transaction facilitators. This framework does not provide a model for all current transactions. For example, many cyberspace transactions are not so "commercial": In many Web browsing transactions, neither server nor client is exchanging information to turn a profit, and no payment provider is involved. Think of the many Web sites we browse to gather news, financial reports, humor, and scholarship – all without payment. Further, this architecture cannot model all future cyberspace transactions; their diversity defies prediction. For example, there may be numerous transacting parties in complex, multilateral deals. There may be other types of transaction facilitators, such as time-stamp authorities, n196 certification authorities, n197 anonymous remailers, n198 and electronic malls that handle accounting, shipping, and inventory for their merchandisers. Indeed, some of these facilitators may operate without ongoing human intervention; rather, they may be pieces of advanced software or "intelligent agents." n199 To complicate matters further, the distinction between transaction facilitators and transacting parties – already hazy in many cases – may dissolve further as merchandisers, communications providers, and payment providers vertically integrate. Nevertheless, the architecture provides a useful vocabulary, [*1238] one that connotes the magnitude and complexity of personal information triggered by quotidian cyberspace transactions.

C. Data Mining

As cyberspace becomes the preferred medium to complete the day's innumerable tasks, it will generate for each individual a mother lode of personal information, recorded dutifully – and often invisibly – by computers that know no sleep. These tasks include not only the sort of cyber-commerce that my software purchase example illustrates. They also include the plain old reading, e.g., for research, entertainment, or current awareness, of the Web pages we browse. They include each and every communication we have with friends, colleagues, organizations, and governmental agencies. They include interactions with pharmacists, financial institutions, and political parties. This mother lode of personal information will be mined for all its value. n200 The postindustrial economy generally and the telecommunications sectors particularly are seeing increased competition. This will prompt firms to exploit every competitive advantage, including the use of personal information.

For instance, firms may create entirely new revenue generating services from the manipulation of personal information, such as Caller ID. n201 Or firms may collect and process personal information to insure that they receive full payment for the consumption of copyrighted goods. n202 Or, less creatively, firms may find marketing uses for personal information, as they enter lines of business previously forbidden. n203 For example, most LECs currently use customer toll records only to route calls and bill customers. But as LECs begin to enter the long-distance market, as the Telecommunications Act of 1996 allows, n204 they will face increased incentives to use this toll record information for marketing their own long-distance services. n205

[*1239] The consumption preferences and behavioral patterns of individuals – as revealed by cyber-activity – will be widely used for database marketing. n206 This form of marketing is premised on the fact that the more information one has about a potential consumer, the easier it is to target advertisements for products and services to that person. A sophisticated database marketing initiative thus acquires as much data on potential customers as legally possible. n207 Through database marketing, firms can now generate surprisingly detailed personal profiles. n208 When such data are overlaid onto specific transactional data generated by cyberspace transactions – what we read, what [*1240] we view, what we buy, to whom we speak – a rich and telling portrait of the individual is possible. n209

These portraits have substantial economic value, and developers of advanced interactive networks have already expressed keen interest in wedding database marketing to cyberspace. n210 Moreover, such portraits pose a synergistic threat to privacy – synergistic in that the privacy threat of the profile is greater than the sum of the privacy threats associated with each individual bit of information considered in isolation. n211 In the near future, then, we may witness what Gary Marx has predicted:

Purchasers of pregnancy-testing kits may receive solicitations from pro-and anti-abortion groups Purchasers of weight-loss products or participants in diet programs may be targeted for promotional offers from sellers of candy, cookies and ice cream, or, conversely, those whose purchases of the latter exceed the average may receive offers for weight-loss products and services. Subscribers to gay and lesbian publications may be targeted by religious and therapeutic organizations, or face employment denials, harassment, and even blackmail. Frequent travelers and those with multiple residences may receive [*1241] solicitations from sellers of home-security products, and such lists would be a boon to sophisticated burglars. A list of tobacco users might be of interest to potential employers and insurance companies. n212

For some, this data processing raises nary an eyebrow; for others, it shocks the conscience. Who is right, and how do we decide?

D. Encryption

Before trying to answer these questions, an aside on technology is warranted. Above, I described how the new technologies of cyberspace threaten privacy. A balanced view also requires an understanding of how new technologies can protect privacy. n213

1. Possibilities.

The principal privacy-protecting technology is encryption. In basic terms, encryption uses a cryptographic algorithm and a key to encode a message - plaintext - into something incomprehensibly garbled - ciphertext. Once communicated to the intended recipient, the ciphertext is decoded back into plaintext. If the cryptographic algorithm is strong, and the key properly selected and kept secret, it is infeasible for an unauthorized party to intercept the ciphertext and decrypt it back into plaintext. This basic concept of encryption lies at the heart of multiple privacy-promoting technologies. n214