An Infomediary Approach to the Privacy Problem

by Fen Labalme[1] and Jad Duwaik

February 1999

Table of Contents

Introduction....1
What Is Privacy? 2
Widespread Concerns About Privacy 2
Why Do Companies Violate Privacy? 5
Fair Information Principles 6
The European Union Privacy Directive 9
Lumeria - Your Privacy Partner 10
Lumeria Introduces I-Commerce 12
Evolution of the SuperProfile System 16
Conclusion: A Win-Win-Win Situation 17
Lumeria's Privacy Statement 19

Introduction

As opposed to mass marketing to a faceless audience, direct marketing sends a message to an individual or group of individuals. The power of direct marketing is that the advertiser attempts to send her message to only those people who want or need her company's product or service. In order to accomplish this objective, however, the advertiser must have knowledge of her audience, both those included and excluded in the message.

Consequently, over the last thirty years, direct marketers have been gathering extensive information about individuals which was used to reduce unwanted mail. This admirable goal was accomplished, however, without the individual's involvement or consent as third party entities collected, managed, rented, traded, and exploited the value of their data with nary a word mentioned to the individual. In fact, in 1995, a direct marketing trade magazine featured an article titled, *Dumbing Down What We Know: How to Use Data without Scaring Your Customers*.

Lumeria plans to obliterate this antiquated business model and create an environment in which individuals and marketers can collaborate together to satisfy each other's goals while respecting an individual's right to privacy. Please see the Conclusion for more information about the benefits of the SuperProfile system to users, marketers, and merchants.

1 Fen was V.P. of Technology at Lumeria, co-founder of OpenPrivacy <http://openprivacy.org/> and is currently (2004) CTO of Identity Commons <http://identitycommons.net/>.

What Is Privacy?

The specter of George Orwell's 1984 is once again rearing its ugly head. After revolutionizing the world of telecommunications, the Internet is poised to take the next step toward ubiquity. And, with it, the Internet presents the ability to track and monitor the individual in a manner that is eerily similar to the world represented in 1984.

Many companies are attempting to connect all sorts of devices to the Internet. Although their products will provide a wealth of additional services, few have realized the consequences. Namely, when every electronic device is connected to the Internet, a person can be monitored as they drive their car, use their stereo or TV, or open the refrigerator. In short, their privacy can be (or, as many people already believe, has been) obliterated.

But, what is privacy? In the Internet age, the definition of privacy provided by Alan Westin in Privacy and Freedom seems most fitting:

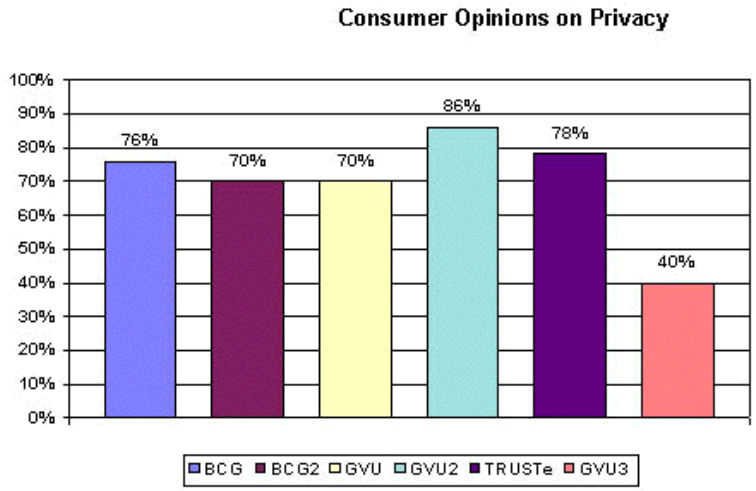
> "*the claim of individuals, groups, or institutions to determine for themselves when,*
> *how, and to what extent information about them is communicated to others.*"

Whereas privacy issues used to apply to what Chief Justice Brandeis called "the right to be left alone," Lumeria believes that privacy is not about hiding from others, but rather about controlling the flow of your personal data. For example, if you walk into Wal-Mart and the greeter at the front door calls you by your name, are you more concerned about this stranger knowing your name or the method in which your name (and possibly other information) was appropriated without your knowledge?

Widespread Concerns About Privacy

In the marketplace, companies have routinely had access to better information and better resources which has generally been leveraged against the individual. However, until the last 50 years, the economy was based on manufacturing and so information was an influential factor, but not a product, in and of itself. Consequently, information gathering was a peripheral activity.

Times have changed. The explosion of the Internet demonstrates the power and value of information (which has garnered center stage) and has led to frequent abuses of privacy including corporate espionage, reconnaissance, and counterintelligence missions of consumers, competitors, and suppliers. As the value of information continues to increase, these abuses will remain unabated and consumers will be increasingly hostile to information requests. In fact, surveys have shown that privacy is already a highly sensitive issue on the Internet and a potential impediment for e-commerce.



BCG - A BCG Consumer Survey of users who expressed concern over Web sites monitoring their browsing habits	GVU2 - The same survey of consumers who expressed a desire to control use of their demographic information.
BCG2 - The same survey of users who expressed concern about making purchases online.	TRUSTe - TRUSTe's survey of individuals who said they would be more likely to provide information to Web sites that provided privacy guarantees.
GVU - An annual Web survey conducted by the Graphics, Visualization and Usability Center of the Georgia Institute of Technology shows consumers who cited privacy concerns as their primary reason for not registering demographic information with Web sites on the Internet.	GVU3 - Another Georgia Tech study of users who reported providing false information at least once while registering at a web site.

These surveys suggest that individuals have strong concerns about a company's use of personal data. This fear is well grounded. Businesses are in business to produce profit and it is difficult to resist the temptation to use personal data that could create additional revenue. The following list (in part provided by John Hagel and Marc Singer in their book, Net Worth) catalogs a few samples of privacy breaches.

- The web site GeoCities suffered a 15 percent drop in the market value of its stock after settling charges with the Federal Trade Commission that it had been secretly selling personal information to marketers. GeoCities maintains that nothing illegal was done. Immoral or unethical, perhaps, but definitely not illegal.
- Pacific Bell, either ignorant or blatantly apathetic, wanted to send unsolicited sales pitches to customers with unlisted phone numbers. PacBell seems to be saying you can run, but you can't hide.
- Internet behemoth America Online sold its members' phone numbers (without consent) to a telemarketing company. In an unrelated event, AOL turned over personal data about an individual's sexual preferences to the U.S. Navy without the individual's consent. AOL's motto: don't ask, but we'll tell.
- Financial services giant American Express announced plans to sell extensive information on its cardholders to merchants. This data is like a pile of cash sitting in the corner. Other companies are reaping the rewards, so why can't AmEx do it, too?
- Smaller companies can get into the act, too. Blizzard Entertainment admitted it had acquired data (again without consent) from its customers' PCs via the Internet. How's that for interactive entertainment?
- Giant Foods (a supermarket chain) and CVS (a drugstore chain) shared medical information with a drug marketer who sent out friendly prescription reminders and helpful literature about new drugs. Now the friendly and helpful mailman knows your medical history.
- GTE accidentally published 50,000 unlisted phone numbers and addresses. However, GTE expressed its deepest apology over the incident so it shouldn't be held legally or morally responsible for the consequences to the personal safety of police officers and crime victims who had this information unexpectedly divulged.
- Microsoft acknowledged that their Office software products utilized a serial number that could be used to trace every document an individual creates. TRUSTe, the industry watchdog that is partly financed by Microsoft, firmly admonished Microsoft and politely asked the company to refrain from similar behavior in the future.
- In an attempt to support e-commerce, Intel announced a plan to place serial numbers in its Pentium chips. An enormous privacy backlash convinced Intel to provide software that could turn this wonderful feature off. However, a hacker demonstrated that this feature could be remotely turned on without the user's knowledge. Perhaps the software simply experienced a floating point error.
- In response to the Intel debacle, Sun Microsystems CEO Scott McNealy said, "You have no privacy. Get over it." Perhaps, two hundred years ago, Benedict Arnold had similar comments about British oppression.

Privacy, as defined by Brandeis, is not the solution. Individuals want to share their personal data in order to benefit from personalized services, screen out unwanted advertisements and to find out about new products (especially from competitors) for which they have an interest. However, individuals also want control over their personal data. Moreover, they want to be compensated by marketers for their increasingly valuable time.

Why Do Companies Violate Privacy?

A profit driven company will only pursue activities in which the net benefit is positive. Consequently, despite the privacy backlash against companies, there is obviously a positive return from the acquisition of personal data for direct marketing. In fact, this process is simply driven by the desire to screen out unlikely candidates from a marketing message.

This innocuous objective would seem likely to be greeted with enthusiasm from consumers. Unfortunately, the theory is not as pure as the execution. First, even a highly targeted direct marketing piece will only receive a 25-30 percent success rate, i.e. two out of three individuals are still receiving an unwanted advertisement. Secondly, individuals are more concerned with how a marketer attained their personal data rather than the fact that it has been attained. This is the breach of privacy: the individual has no knowledge or control of this flow of data. He cannot access the information, he cannot change the information, and he cannot delete the information -- even if he would like to correct inaccurate information to help the advertiser screen him out!

Many times, a company's acquisition of personal data is not initially perceived to be a violation of privacy. Consumers routinely provide information to companies with the expectation of receiving personalized services or shopping discounts. In fact, this personalized, one-to-one marketing is one of the most attractive promises held out by Internet technologies. However, the data's inherent value creates an seductive temptation to abuse the consumer's trust and utilize the data for other purposes (which GeoCities allegedly did).

Self-regulatory Initiatives

Self-regulatory proposals, such as TRUSTe and BBBOnLine, attempt to muzzle this temptation. However, the responsibility for privacy assurances sits in the hands of each Web site - designating the proverbial fox to guard the hen house. As Fred Davis, CEO of Lumeria puts it, "In the morning, the hens have disappeared, there's blood and feathers everywhere, and the foxes blithely state that the alarms didn't go off so there must not be a problem."

The Federal Trade Commission, the European Union, and the entire privacy community have noted that these systems offer minimal recourse beyond the Web site owner. The underlying problem is that a company's privacy policy is not legally binding. (In fact, some privacy advocates suggest that privacy policies are legal disclaimers!)

Consequently, neither the government nor any other third party entity can step in to assist the individual. Moreover, even the self-regulatory organizations have demonstrated their impotence. For example, after the recent discovery that Microsoft software could track every document a user creates, TRUSTe (which receives considerable funding from Microsoft) concluded that the breach of privacy was not web site related and therefore Microsoft did not violate the terms of its license with TRUSTe.

Fair Information Principles

In 1998, the Federal Trade Commission (FTC) conducted a study of 1,400 web sites and found that only 14 percent possessed a privacy policy that explained to consumers what might happen with their personal data. The following five sections are copied directly from this study, Privacy Online: A Report to Congress. The FTC expounded these Fair Information Principles as a foundation that should be the basis of any self-regulatory process or privacy policy creation. The entire document can be found at http://www.ftc.gov/reports/privacy3.

1. Notice/Awareness

> The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles discussed below -- choice/consent, access/participation, and enforcement/redress -- are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.
>
> While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:
>
> - identification of the entity collecting the data;
> - identification of the uses to which the data will be put;
> - identification of any potential recipients of the data;
> - the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);
> - whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
> - the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data; whether the consumer has been given a right of access to the data; the ability of the consumer to contest inaccuracies; the availability of redress for violations of the practice code; and how such rights can be exercised.

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any Web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

2. Choice/Consent

The second widely-accepted core principle of fair information practice is consumer choice or consent. At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information -- i.e., uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer. Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put. Thus, for example, consumers can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their

preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.

3. Access/Participation

Access is the third core principle. It refers to an individual's ability both to access data about him or herself -- i.e., to view the data in an entity's files -- and to contest that data's accuracy and completeness. Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.

4. Integrity/Security

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.

5. Enforcement/Redress

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles.

The European Union Privacy Directive

In October, 1998, the European Union (EU) adopted the Directive on Data Protection which sets forth strict rules for companies which handle personal data about EU citizens. This restriction includes US companies because of a small provision which prevents the transfer of data to any country which does not have "an adequate level of privacy." The US and EU are currently in discussions over how to best resolve the situation in which a ban on enforcement of the noted provision has been postponed numerous times. The US is seeking to allow industry to self-regulate, however, there have not been sufficient advances in its development to alleviate the EU's concerns about privacy abuse.

Specifically, the EU Directive includes the following elements:

- Companies must notify both employees and consumers about how information collected about them will be used;
- Companies can only use data for its intended purpose;
- Companies cannot transfer data on employees and consumers to countries with inadequate privacy protection laws;
- Consumers will have a right to access data collected about them;
- Consumers will have a right to have inaccurate data rectified;
- Consumers will have a right to know the origin of data about them (if this information is available);
- Consumers will have a right of recourse in the event of unlawful processing of data about them;
- Consumers will have a right to withhold permission to use their data (e.g. the right to opt-out of direct marketing campaigns for free without providing a reason);
- Companies need explicit permission of consumers to process sensitive information, including information on racial origin, political or religious beliefs, trade union membership, medical data, and sexual life.

According to Gerard de Graaf, a member of the European negotiating team with the US, "We would not accept a situation where the only way to deal with a problem is to sort it out with the company that is the root of the problem in the first place." In addition to enforcement, recent reports suggest that the EU and US currently disagree about the amount of access customers should have to the data companies have collected about them.

The US is currently seeking a self-harbor approach in which individual companies can protect themselves from prosecution by taking certain steps to protect consumer data. If the two governments are unable to reach a compromise, however, the EU could threaten the US with sanctions that could destablize trade relations which currently exceed $300 billion per year.

Lumeria - Your Privacy Partner

Consolidating a person's diversified profile data exponentially amplifies the value of the information, but also its sensitive nature. Consumers are not likely to trust existing companies (who currently possess their personal data) because of their track record of abuse with only nominal amounts of information. The FTC has repeatedly suggested that consumer concern about privacy is the most serious obstacle to the potential growth of e-commerce.

Fortunately, Lumeria is creating some revolutionary technologies and an innovative new business model that will allow them to organize, access and share their own personal data for fun and profit. This model, the SuperProfile system, places personal data under the auspices of the individual and is so robust that it makes the Fair Information Principles as redundant as a friendly reminder to "be careful." Once an individual is empowered with the SuperProfile system, they will no longer be dependent upon the goodwill of the merchant to follow the Fair Information Principles. Nonetheless, these principles provide a foundation for evaluating the potency of the SuperProfile system.

1. Notice/Awareness

> Lumeria's SuperProfile system is based upon the premise that the individual owns their personal data. This seemingly simplistic statement fundamentally alters the principle of notice and awareness. The Federal Trade Commission advocates that the user be notified of the company's non-binding privacy policy. Lumeria's solution, however, transfers notice and awareness from the company's announced procedures to the binding, contractual terms of the exchange. The company's privacy policy becomes irrelevant because the individual can negotiate the limitations on the use of the data. If, for example, the consumer is concerned about the usage of data beyond the immediate exchange, then they can specify that the purchase of the data includes only a single usage. Similar restrictions can be placed on any aspect of the acquisition, control, or use of the data and Lumeria's SuperProfile system provides the tools necessary to insure that the individual can enforce these terms.
>
> Obviously, the terms of the exchange can continue to be constructed in such a way as to exploit a person's data. However, the SuperProfile system allows individuals to appoint agents (such as Lumeria or other third parties including banks) who will actively seek the best deals for the individual. The agent can provide software that highlights deficiencies of any transaction or warns the individual about a scrupulous deal. Moreover, the SuperProfile system allows the individual to sell or trade some data about themselves (e.g. their habits or preferences) while protecting their identity. If the individual suspects the veracity of the company, they can provide extremely limited or anonymous

data to the company until a relationship has been established and the merchant is trusted.

2. Choice/Consent

Once Lumeria has given the individual control over the exchange of their personal data, secondary usage become part of the contract. If the individual trusts the party, they can provide secondary usage of the data (i.e. their name for personalized services in the future) but limit its transferability to any other entity. Also, since the provision of data becomes a contractual exchange, the assumption is that the individual has a choice about participating.

3. Access/Participation

Personal ownership of an individual's data dictates that the individual has access to their property. The data's inherent value also suggests that the individual will actively maintain the data's accuracy and seek additional information to add to their SuperProfile. Because the individual owns this data, they can individually determine whether to restrict, delete, or publish this data.

4. Integrity/Security

As mentioned above, integrity of the data is easier to maintain once the individual has incentive to maintain its accuracy. Using digital certificates, Lumeria's SuperProfile system provides the tools necessary for an individual to authenticate or audit specific data, thereby increasing its value (e.g. the consumer can provide audited or unaudited information). In addition, the SuperProfile system utilizes double-blind verification, reputations, strong encryption, and redundant backup to create a secure, trusted system.

5. Enforcement/Redress

The enforcement principle is Lumeria's strong card. Privacy is difficult to enforce today because there are few specifically designated privacy laws. The Constitution, for example, does not use the word privacy. Moreover, the privacy policy of a company is not a contract and is rarely binding. Lumeria's SuperProfile system, however, converts ephemeral personal data into an asset property. When either an individual or a company utilizes the SuperProfile system, the terms and conditions of participation become a legally binding contract. This contract is then enforceable by any court of law utilizing existing contractual law. (Although few countries have privacy laws, almost all countries have a robust contract law foundation.)

6. Addressing the EU's Concerns

Although the Europeans are considered to have some of the strongest privacy laws in the world (some EU countries can prosecute some breaches of privacy under criminal laws), the SuperProfile system would actually exceed EU guidelines in many areas. For example, the EU Directive does not allow for anonymous web surfing or e-commerce purchases. In addition, access to personal data is considerably easier when it's consolidated under the SuperProfile, rather than having to contact multiple companies to request the data. Most importantly, the EU Directive does not consider personal data to be the property of the individual. Consequently, the EU only protects personal data, but does not provide, like Lumeria's solutions, the numerous benefits from sharing your data with others (i.e. direct compensation, discounts, and additional services).

Lumeria Introduces I-Commerce

In a recent no-action letter, the Securities & Exchange Commission (SEC) opined that a company was selling stock if the company received personal information (i.e. a name and address) as compensation for the stock. The SEC's recognition that personal data has value has long been recognized by list brokers who have amalgamated colossal databases of personal information in order to drive the $175 billion direct marketing industry.

Technology is revolutionizing this industry because it has drastically reduced the cost of acquiring and managing information and created a new medium, the Internet, in which producers and consumers can interact. This has created the possibility of new business models to personalize e-commerce services and offer one-to-one direct marketing. However, while the hard costs for acquiring data have been reduced, the social costs have increased. Most of the currently proposed personal data management solutions ignore these costs and have inflamed the debate on personal privacy.

Lumeria's SuperProfile system, which minimizes these social costs by offering a complete privacy solution, creates a revolutionary model that shifts power from companies to the individual. In addition, the SuperProfile system uses personal data as a new form of currency to enable the Identity Commerce marketplace (I-Commerce). I-Commerce is the next step in a number of technologies that have evolved to utilize personal data. Lumeria's solution, however, is likely to receive accolades from privacy advocates and trust from individuals. Lumeria will also kindle the development of I-Commerce in which an individual's identity has a value and can be traded and exchanged for money, discounts, and additional services.

Cookies Technology

On the Internet, the most common profiling mechanism is the "cookie." A cookie is a data file stored on the individual's computer by a specific Web

site. Cookies technology allows a Web site to track transactional information, user preferences, and user activity. Because only the Web site that initially stored the original data can access that data, the individual cannot share any cookie information between different Web sites.

However, it is unlikely that an individual would be interested in sharing this data. Although the data is stored on the individual's computer, the information is stored in a cryptic form such as "cfae017a36014030" which only a computer database can understand. Moreover, most users do not even know what the cookies technology is or how it is used. These users have unwittingly accepted the default option on their browser to accept all cookies requests. Even the minority who has selected the option of verifying cookie requests will generally have difficulty determining what information is being requested. Unfortunately, disabling cookies is an undesirable solution since it results in the loss of the benefits of personalized e-commerce services.

Open Profiling Standard (OPS)

The Open Profiling Standard (OPS) was proposed by Microsoft, Netscape and Firefly. OPS was created in order to provide Internet site developers with a uniform architecture for leveraging profile information to offer individuals customized content while protecting their privacy. OPS was simply a profile or form of an individual's personal data such as name, address, phone number and credit card data. It was initially designed to focus on the secure storage, transport, and control of user data.

However, there were several problems with OPS. First, OPS was still depended upon the support of each Web site in order to be effective (e.g. each site had to be redesigned). In addition, OPS did not create privacy protection beyond the privacy policy of a Web site. Moreover, although OPS was designed to be an open standard, Microsoft's purchase of Firefly discouraged other companies from supporting the standard. Finally, the value proposition to consumers was simply to save time from retyping data. OPS did not attempt to allow individuals to own or profit from their profile.

Platform for Privacy Preferences Project (P3P)

The World Wide Web Consortium (W3C)'s Platform for Privacy Preferences Project (P3P) is an attempt to provide a rich language for the exchange of information between both the user and Web site. In contrast to the one way nature of OPS (from user to Web site), P3P allows the individual to ascertain a Web sites privacy policy before providing her profile data to the site. P3P applications should allow users to be informed about Web site practices, delegate decisions to their computer agent (Web browser, plug-in, or

infomediary agent) when they wish, and tailor relationships with specific sites. Lumeria has announced its support for the P3P protocol.

The Infomediary Revolution

The information intermediary, or infomediary, business model is described by John Hagel and Marc Singer in their book, Net Worth. Published in 1999 by the Harvard Business Press, Net Worth describes this new type of business as an intermediary between consumers and vendors in order to help consumers maximize the value of their personal information. Infomediaries will then act as brokers and agents to represent consumers in commercial transactions and marketing. Although the infomediary model has received consierable attention recently, Lumeria's approach to infomediation has its roots in the broadcatch concepts first developed by Lumeria's VP of Technology, Fen Labalme. Mr. Labalme conceived of broadcatch in 1979 while at MIT in the department now known as The Media Lab.

Traditionally, producers have had greater resources and access to information. This data has been used to refine inventory techniques, maintenance scheduling, and other activities to provide better services to the customer. However, this knowledge has also been used to identify the customer's value drivers. For example, multi-level pricing structures (e.g. peak and non-peak pricing) are a way of extracting greater profit from customers who place a higher value on a given product or service.

Grocery stores and airlines have created membership programs to procure explicit consumer purchasing behavior, which can then be used to pinpoint consumer value and thereby price flexibility. If a consumer demonstrates a strong loyalty to a given brand or a need for specific travel destinations, then prices on those products and services can be raised. Essentially, if a consumer is willing to pay a higher price for a product, then there is a surplus value that the producer has "left on the table." Ideally, a company would like to charge each individual the highest price she is willing to pay in order to extract the entire surplus value from the marketplace.

Whereas technology has traditionally assisted companies in acquiring additional data, the Internet is now flipping this paradigm upside down. Data acquisition techniques, specifically information about competing products, are becoming commonly available to consumers, too. Moreover, producers are finding themselves at an information-disadvantage: companies cannot refuse to share information about their products lest they lose a sale (e.g. a strong supply of product information). Consumers, on the other hand, do not have an intrinsic desire to share their purchasing data with anyone (e.g. a weak supply of purchasing data). Consequently, given a set demand level,

fundamental economics (and experience) dictates that product information will have a minimal value, while consumer data will have a high value.

The infomediary exploits this growing advantage by aggregating consumer data. Although an individual's data, by itself, has nominal value, the combined value of a group of consumers has considerable value to the merchant. The infomediary, representing the individual, enables the extraction of value from the company to the individual. Flipping the picture upside down, the company is willing to pay a higher price for this unique data and has surplus value that the individual can recapture.

The Identity Commerce Marketplace

Simply representing the individual is an evolutionary approach to the Internet economy. Lumeria, on the other hand, intends to take a revolutionary approach. In addition to helping consumers attain compensation for their personal data, Lumeria is developing the SuperProfile system, which will give individuals the ability to:

- opt out of traditional direct marketing programs;
- mask their identities so they can shop online and browse the Web anonymously;
- block cookies requests so that Web sites cannot acquire data outside of the individual's control;
- track their own surfing to build a robust, private profile with user-centric cookie aggregators (as opposed to web site controlled cookies);
- consolidate their various passwords into one password controlled location;
- filter email to delete spam mail;
- pay for e-commerce transactions with electronic wallets that conceal their identity but provide authentication for merchants;
- create a new marketplace for negotiating the use and fees that individuals charge others for the use of their personal data.

The last item, creating the Identity Commerce marketplace (I-Commerce), is the revolutionary step in the SuperProfile system. Fundamentally, the SuperProfile system transfers ownership of personal data back to the individual. Utilizing tools in the SuperProfile system, the individual can then monitor and control the exchange of this data to other parties for personalized services, discounts, or monetary compensation. In other words, the individual participates in I-Commerce, or the new personal data economy.

In addition to merchants, I-Commerce will include marketers and advertisers by allowing them to "buy time" from individuals. For example, an individual could indicate her

interest in purchasing a certain product, such as a new car. Furthermore, she could designate certain data about herself that could assist car marketers in tailoring their sales pitch, or advertisement, to the needs of this individual. The marketer assembles a commercial and an offer, such as rebate or discount, for the individual. Essentially, the marketer pays the individual for her personal data and her willingness to view the commercial.

This is merely one possibility in which a marketer participates in I-Commerce. Another alternative, based on future technologies, is for an individual to download a TV program over the Internet. In exchange for the program, the individual would provide certain data to the content provider or distributor who would use this data to add targeted commercials to the TV program. Under this scenario, numerous people might watch an identical episode of Seinfeld, but each person would see different commercials tailored to their own interests.

The possibilities of I-Commerce are unlimited because I-Commerce is not a closed system with a defined set of rules. Rather, I-Commerce is a set of tools that provides a foundation for a revolutionary economy. Lumeria anticipates that individuals, companies, marketers, and new technology will continue to evolve I-Commerce with new ideas, new concepts, and new products and services to the benefit of all participants. However, I-Commerce will only flourish with the complete privacy solution provided by the SuperProfile system in which an individual has control of their personal data.

Evolution of the SuperProfile System

Once completed, Lumeria's SuperProfile system will exceed the standards of privacy espoused by the Federal Trade Commission and European Union. In fact, our data handling techniques will be modeled after a bank because we feel an individual's personal data is as valuable as money. The SuperProfile system enables the individual to experience:

- a personalized computing environment;
- customized content;
- targeted marketing;
- help in connecting with relevant information and with other people;
- a "spam" management strategy;
- parental control over the use of their children's profiles.

The SuperProfile system will protect an individual's privacy by hiding the details of their activities and using it to generate a profile that can be provided to marketers and merchants. However, Lumeria is anxious to provide specific tools within the SuperProfile system as they become available. Unfortunately, before a complete system can be implemented, these individual tools may not meet the exacting standards we have laid out for our SuperProfile system. Nonetheless, they will probably exceed the precautions that most companies currently undertake.

For this reason, Lumeria will focus on the first two principles: notice and choice. Our

privacy policy will fully describe our data handling techniques and highlight potential deficiencies. We will clearly warn the individual of the risks involved and let the individual decide whether the benefit from the tool exceeds the potential costs.

SuperOptOut

> The first tool that illustrates this issue is the SuperOptOut program, which is designed to help individuals remove their names from existing direct marketing databases. This program also includes an opportunity to "opt-in" to advertisements from which individuals will profit from the use of their personal data by direct marketers. Although both programs will meet most of the Fair Information Principles, there may be some deficiencies (such as the Integrity/Security principle). These issues will be fully disclosed to the individual before she is asked to participate. Then, once informed, she will be given the choice to participate or defer until development of the SuperProfile system is finished. For more information about this program, please see our web site at http://www.SuperProfile.com.

Conclusion: A Win-Win-Win Situation

Consumers will have an obvious interest in Lumeria's technology. The SuperProfile system will offer absolute privacy for those individuals who wish to remain completely anonymous and value to those who are willing to trade their data for direct payment, customized services, or added benefits. Consumers will inevitably feel more comfortable participating in e-commerce once they feel their privacy and the use of their personal data is securely under their control.

Advertisers and marketers (who simply want to communicate their message to individuals likely to respond to their advertisement) will also profit from the SuperProfile system and Identity Commerce (I-Commerce). Every unwanted or ignored advertisement is wasted money for the advertiser. Hence, the marketer invests money in pre-selecting her audience.

This money is given to a list broker, a credit card company, a magazine publisher, or other venue to help the marketer segment her audience. Once segmented, the marketer makes assumptions about each group and chooses a high cost/high impact (e.g. in person visit) or low cost/low impact (e.g. direct mail) approach. Although these assumptions may be efficient for the group, they are unlikely to be the most appropriate technique for each individual.

Lumeria's SuperProfile system allows the marketer to collaborate with each individual by allowing the individual to dictate to the marketer which approach is most efficient. For example, if the individual has minimal interest in the marketer's message, he can indicate his willingness to read an email message for a minimal cost to the marketer. As the individual's interest increases, he can indicate an interest in receiving a higher impact

message (such as a telephone call or drop-in visit) for a higher fee. In fact, as the marketer demands more time and attention from the individual, the individual will expect to be compensated accordingly. I-Commerce gives the marketer the capability to tailor not only her message, but also the medium itself, to the needs and desires of the individual. Hence, both the marketer and the individual will benefit, as the needs of both parties are coordinated.

Merchants and Web sites will also profit from Lumeria's SuperProfile system. Individual companies, such as grocery stores and airlines, already collect personal data about their customers. The purpose of this data collection is to identify profitable customers. However, each company is unable to determine the individual's spending with that company as a percentage of his total spending for a given category (e.g. how much is the customer spending with competitors). This critical piece of data, available with the I-Commerce system and the individual's consent, can help a company to identify revenue growth opportunities with individuals who have additional demand for a given category but currently spend that with competitors.

Finally, many companies collect large amounts of data about its customers, but are unable to extract meaningful conclusions from the morass of bits and bytes. Lumeria's focus on personal data will help advertisers and merchants better understand what data they need and don't need. Also, much of this data is collected today at minimal cost and so companies have not found a need to prioritize the data. With Lumeria's business model, every additional byte will have a cost - paid to the individual - and therefore encourage companies to identify the value of the data received to insure a net positive return.

Lumeria's Privacy Statement

The next decade will be a critical period in the development and articulation of the individual's right to privacy in American society and the world. In *Privacy & Freedom*, Alan Westin offers the following definition for privacy:

> *"Individuals, groups, or institutions have the right to control, edit, manage, and delete information about them and decide when, how, and to what extent that information is communicated to others."*

Using Westin's definition as a beacon, we are committed to developing technologies to insure that individuals are not trampled for the perceived short-term benefit of corporate, governmental, and/or marketing interests. Furthermore, privacy is not just about hiding information from others, but also controlling the flow of your personal information. Your personal data should be your property. We are developing tools necessary to help you manage, control, and protect this property. However, this is an extremely broad definition of privacy that does not take into account other societal values.

Sometimes, for example, individual privacy must be compromised for the public good. In *Privacy in the Information Age*, author Fred Cate offers the following examples:

> *"What parent would not want to know if her child's babysitter had been convicted for child abuse? Similarly, what store owner would not want to know whether a clerk was a kleptomaniac? What patient would not want to know whether his physician had a history of malpractice? What man or woman would not want to know if a potential sex partner had a sexually transmitted disease? What airline would not want to know if its pilots were subject to epileptic seizures?"*

The answers to these questions, provided by our government, society, and you, may dictate that some of your personal data must be made available. Lumeria will provide the tools to help you comply with these requirements, but inevitably, the responsibility will fall upon the shoulder of the individual. Ultimately, Lumeria's system will be designed such that even Lumeria, and its employees, will not have access to your data without your consent. Consequently, if the government subpoenas your information, Lumeria would only be able to turn over garbage without your key to decrypt it.

As a general statement of business policy, we believe that the individual's right to privacy includes the ability

- to view, in its entirety, the information collected about its owner;
- to delete the information collected;
- to identify every entity (especially when that entity comes into contact with the individual) who has accessed, or has access to, the information and their stated purpose for doing so;
- to determine who will and will not have access to this information;
- to derive value from the use of this information.

Please keep in mind that in any transaction or conversation with another entity, the merchant or other party has an equal right to the transaction's information as you. Although many transactions can be conducted anonymously, your right to privacy does not extend to controlling whatever data to which the other party has access unless all parties involved have previously established an agreement about how the data can be used.

Finally, as of today, there is an enormous amount of data about you that exists in the hands of the government, insurers, hospitals, banks, publishers, list brokers, and much, much more that is not currently your property and which you may not be able to control, manage, or receive any benefit. Unlike Big Brother in 1984, we cannot change the past, only the future.