Towards Markets for Personal Information

Rachel Greenstadt, Michael D. Smith
{*greenie,smith*}*@eecs.harvard.edu*
Harvard University

January 26, 2004

Abstract

Economists have proposed to give individuals property rights over their personal information, allowing individuals to exert control over how the information collected about them is used and distributed. In this paper, we look at a recently repealed Oregon state law and a range of other market proposals. For each, we discuss where they address and fall short of solving the privacy problem in the United States, identifying legal, social, and technical challenges which must be overcome to produce functioning markets for personal information. We suggest ways to combine elements of these proposals and add new elements to create a viable market structure for personal information, and we propose methods of enforcing the fair operation of these markets.

Keywords: privacy, information economics, markets, property rights, data aggregation

1 Introduction

The concept of personal information as property right has been proposed as a potential solution to privacy problems in the United States. Recent survey data indicates that 92% of consumers are concerned about the misuse of their personal information gathered while online [5], and that such privacy concerns are the number one reason why individuals choose to stay off the Internet [13]. Treating personal information as property implies a market for that information, and in this paper, we investigate questions of whether such markets could address current privacy concerns and how they could put control of personal information back in the hands of individuals.

The term "property rights" generally refers to two types of rights: possessory rights and rights of transfer [23]. Possessory rights are rights to use

things and to prevent others from using them. The right of transfer is the right to give a possessory right to someone else. A distinct but similar right is that of the recipient to then transfer the possessory right further.

If individuals wanted to use these rights to control the flow of information about them, then they should not transfer these rights to others, but rather use their possessory rights as a tool to control the information and grant rights of use of the information to others under licensing terms. Property is a well understood concept in law which allows a stakeholder to control that property. It also allows information to flow if the price is right, which may result in a social good.

The contribution of this paper is in the identification and analysis of challenges to implementing and enforcing fair markets for privacy. This question has only been addressed in a cursory manner in the literature. We argue that the obstacles to creating markets are significant, but identify areas of research that may overcome these pitfalls. This problem has many pieces. We present a framework for further research into privacy markets.

We seek to answer a number of questions about these markets. Are these information markets useful? What sort of technical, social, and legal[1] barriers lie in the way of their implementation and usefulness? How should the market be structured?

These questions are difficult to answer because privacy is a slippery design goal and privacy invasion a vexing social problem. In particular, privacy invasion means different things to different people [25]. For some privacy invasion means being annoyed, as in receiving spam or telemarketing calls. To others it might mean being embarrassed when browsing habits or compromising data are made available to strangers. Still others believe it means being overcharged for an item because a company is price discriminating against them based on knowledge of their personal information. Among the most pressing privacy concerns is that sloppy handling of personal information can lead to identity theft. In general, there is no universal standard for handling personal information that will satisfy everyone and no bright line separating our truly private information from the rest of our personal information.

The computer science community first attempted to address the privacy problem by creating tools based on anonymity and cryptography that help individuals keep personal information private. Though these techniques can help an individuals hide their personal information, the techniques alone

[1]When discussing legal issues, we present a United-States-centric view by virtue of familiarity. An international perspective might be useful but is not presented here.

cannot help individuals control or regain control of their information once it has been disclosed. To reduce the likelihood of unauthorized disclosure by unscrupulous companies or organizations, tools like P3P [18] were designed to help individuals determine which companies could be trusted to protect their personal information. Unfortunately, the industry has resisted measures which make it easier to determine which entities can be trusted: an economic analysis of the situation shows that corporations lack incentives for properly informing users about corporate use of personal information [26]. Regulations such as California SB 1386[2] are a step toward better alignment and protection of personal data, but these laws still not a solution to putting control of personal data back in the hands of individuals.

Section 2 characterizes markets for personal information and describes the full set of technical, social, and legal challenges that these markets face. Section 3 is a brief case study focusing on a recently repealed Oregon law that declared an individual's genetic information to be the property of that individual. The Oregon law demonstrates the difficulties of a market-based approach to privacy and highlights some of the obstacles any solution will encounter in dealing with personal information as a property right. Sections 4 and 5 examine two proposed markets for personal information. Section 4 examines the National Information Market solution proposed by Kenneth Laudon [16], while Section 5 discusses a decentralized approach to the market proposed by Adar and Huberman [1]. We examine the feasibility of these proposals from a technical and social perspective. By considering these proposals together and looking at them in light of practical, technical considerations new insights emerge about viability of these proposed solutions and the privacy space in general. Section 6 discusses what is needed in order to make an information market meaningful, Section 7 provides a framework for further research and Section 8 concludes with statements about the potential of these markets.

2 Markets for Privacy

When electronic privacy issues started to receive attention, many economists feared that either private information would be restrictively protected by reactionary legislation or rampantly abused [16, 25]. As a middle ground, they

[2]This measure mandates that any corporation doing business in California and maintaining personal information on California residents publicly disclose all computer-security breaches where any California resident's personal information may have been compromised.

proposed enshrining privacy rights in the hands of individuals [1, 16, 20, 25]. They reasoned that the problem with privacy in electronic markets today is that there exist third parties who collate and sell private information. Individuals suffer a cost from these transactions, but they do not get to participate in the market. This negative externality results in the privacy problems witnessed. Many individuals might be willing to give up certain information about themselves if they were compensated. In turn, the cost of using personal data would rise and there would be more privacy in society as a whole as firms would likely reduce the amount of information they collect. In order to facilitate the fair and legal transfer of information, economists have proposed a market for information. That market might be either centrally adminstered by the government or decentralized and anonymous.

There are a number of difficult challenges that must be faced before these markets are feasible. If privacy is a fundamental right, protected by the U.S. Constitution, it should not be legal to sell this right, regardless of whether it is being violated already. There is no explicit right to privacy stated in the constitution, but the Supreme Court has found support for such a right in the 1st, 4th, 5th, 9th and 14th amendments [16]. A market might cause privacy divide between the rich and poor. The rich will be able to afford the *luxury* of privacy while the poor may be forced by economic necessity to sell their very identities. If a right to privacy exists, then there is a moral hazard here. However, this is an arguable point because the personal information of wealthy individuals may be worth more.

There are also political challenges involved in implementing this market. Businesses benefit from the status quo and like to be self-regulated. They benefit from the externality which this market might correct. Since these businesses have substantial lobbying power it is unlikely that the laws which might enshrine information property rights in individual hands will pass without significant public demand for privacy. So far such public demand for privacy regulation has not materialized. Even if such laws are passed, they will surely be challenged in the courts. We are not lawyers so these legal and political challenges are outside the scope of this paper. Nonetheless, they must be dealt with if market-based approaches to personal information are to succeed.

However, there are significant challenges in enforcing the fair operation of this market that we do address. For the individual selling information, the mechanism has to ensure that the information is acquired legally and paid for. For the entity buying information, it is important to ensure that they are buying accurate information. Today, many consumers lie about personal information in order to maintain privacy. This problem would be

exacerbated if payoffs varied based on the perceived value of the information as in Kleinberg *et al*'s 'On the Value of Information [15].'

3 Case Study: Oregon

There has really only been one law which attempted to give individuals property rights to their personal information. This was an Oregon state law (ORS 677.097) passed in 1995. During the years that the law was on the books, it was never challenged in court. As a result, it did not provide any precedent regarding the legal issues discussed in the previous section. The relevant clause read, "An individual's genetic information and DNA sample are the property of the individual except when the information or sample is used in anonymous research (the identity of the person from whom the sample is derived cannot be determined) [12]." In 2001, Oregon Senate Bill 114 repealed the law, replacing it with penalties for misuse of DNA information. This decision was based on the recommendation of the Genetic Research Advisory Committee(GRAC) which consisted of representatives from the legislature, health care industry, pharmaceutical industry and business and consumer affairs [21]. Genetic privacy is an interesting case to study, because there are clearly important privacy concerns involved, but also clearly a great public good can be accomplished by allowing this information to flow appropriately.

The GRAC cited three reasons why the property clause was included in the first place.

- It's a simple concept.
- It gives families ownership of the genetic material of a descendant.
- It provides families with protection from discrimination by providing them with standing for legal action.

The majority of the opposition to the law came from the drug industry. It is illustrative to look at the criticism of the law.

- Obtaining consent from individuals for the use of their DNA is slow, costly, and sometimes impossible. As such it inhibits important genetic research.
- The law makes genetic privacy an alienable right which can be sold, leaving the individual with no recourse and no control over their information. Perhaps it is possible to license DNA to firms but not sell one's property rights completely, but there was no discussion of this and no mechanism for it in the law.

- No one knew how property rights should be obtained. Did a firm need to obtain consent from individuals to use their DNA? Did individuals whose DNA was used maintain an interest in any drug or treatment developed based on their genetic material?
- Genetic information cannot clearly belong to a single person, as blood relatives (especially identical twins) share that genetic information and therefore are entitled to some control over it.
- The committee members felt that individuals were more interested in control of their DNA and protections against misuse than in obtaining monetary gain from their genetic information. As a result, data protection laws might provide adequate protection.

A lesson from Oregon's experience is that property rights alone are not enough. Most of the criticism of the law amounted to opposition to its ambiguity. Corporations did not know what their liability was and there was no market structure in which they could easily and unambiguously obtain the rights or licenses needed to legally do their research. There was no way for corporations to opt to do research using anonymized DNA. The situation in Oregon demonstrates the need for a market structure in which property rights for DNA or any other regulated personal information can be meaningful.

4 A National Information Market

Kenneth Laudon was among the first to describe a market for private information. He envisioned a national information market overseen by a Federal Information Commission much like the SEC. People would retain property rights tied to an account number that could be managed by a local bank. The banks could aggregate information according to similar demographics to both aid in privacy and provide greater value. When anyone wanted to use the information for a secondary purpose (outside of the normal information required to do business) they would need to acquire the approval of the owner of that information (the identity it was tied to) and pay them a fee. The FIC would track the market and make sure that information was not transferred for other purposes. A diagram of this market is presented in Figure 1.

In the Laudon market, information is sold for a specific purpose and further sales or secondary uses are prohibited. This creates the problem that the use of information must be carefully audited and tracked in order to enforce the fair operation of the market. This is a very difficult problem.

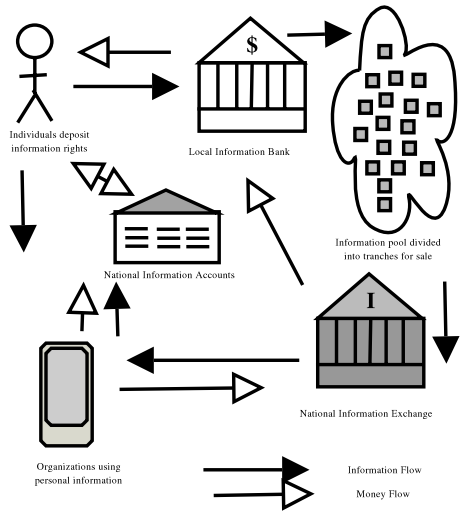

Figure 1: How a National Information Market would work [16]

Laudon's solution is that the FIC will solve it. His paper does not address how.

We see two potential facets of any approach to solving it: (1) enforce the fair operation of the market using technology and (2) enforce the fair operation of the market using laws and policies. Any viable solution will use both technology and policy. As Bruce Schneier is fond of saying,

> "In the real world, security involves processes. It involves preventative technologies, but also detection and reaction processes, and an entire forensics system to hunt down and prosecute the guilty [22]."

4.1 Technological Approaches to Enforcing the National Information Market

Information in the digital age is cheap and easy to copy. Controlling information property is analogous to controlling intellectual property, otherwise known as digital rights management in the entertainment industry. Measures to control information require either technology that currently does not exist or draconian tracking of information likely to drastically reduce the privacy of the individual even as it attempts to increase it.

It is useful to look to the field of digital rights management to see what tools the market might use to restrict access to data. One of the principal

tools being researched by that industry is watermarking, along with fingerprinting and other information hiding techniques. Watermarking is the practice of embedding a mark into a piece of content that is difficult to remove and that can be used to track it [7]. Recent advances in watermarking technology have enabled traitor tracing techniques that customize information to the holder, thus enabling discovery of the "traitor" who illicitly leaked the material [14].

The industry is also investigating the use of secure hardware that can certify the software on top of it and protect storage from the user. Information could then be given to a data miner's machine which could only be read by approved and certified software. This software would then ensure that the information was not used inappropriately [17, 24]. Consumers fear these changes may reduce their ability to use their computers as they please and to share copyrighted content within fair use laws.

These techniques may effectively raise the cost of distributing information illegally. However, sensitive and personally identifiable items like social security numbers and credit card numbers are surely easy to copy, as anyone who sees them can write them down on a piece of paper. One possible answer to this is to require information holders to have a license to possess that information from its owner [6]. Then offenders can be sued if they are found to illegally possess information.

In this market, businesses are allowed to collect information for primary use and the government is needed to monitor and track secondary uses of information. This is likely to be very difficult and require extensive and intrusive monitoring. It will give the government a comprehensive database of where what information is stored about all citizens. Such a database would be extremely useful to law enforcement and no doubt would be utilized by them. This seems like more privacy invasion than what we have now.

4.2 Policy Approaches to Enforcing the National Information Market

Even though it may be impossibly difficult to prevent abuses of a centralized National Information Market, society might be able to limit them through legal action. For example, a firm that abuses the private information of individuals may be subject to a class action lawsuit and forced to pay penalties. If these penalties were sufficiently high, draconian measures to prevent abuse might be unnecessary.

There is also a strong possibility that the legal system can utilize watermarking and traitor tracing techniques for legal action. Plaintiffs may

be able to use the Digital Millenium Copyright Act (DMCA), or something like it, to claim damages against firms which circumvent technology used to protect their private information. The concept of data licenses may prove particularly useful because the information regulated is often of a personal nature and easily linked to a human being. That human can then claim damages against any entity which uses that information without an appropriate license.

However, in order to pursue legal action, individuals will need to identify the offender. This is likely to prove difficult. The majority of victims of identity theft do not know how their information was lost. Often they do not even realize they are victims. If there is a strong probability of getting away with abusing the National Information Market, it will not be an effective mechanism for giving individuals control over their information. A strong auditing mechanism is absolutely essential for the functioning of this market.

5 A Decentralized Market for Secrets

Another proposed model for information markets is a decentralized mechanism known as Information Crystals [1]. This mechanism utilizes pieces of encrypted, mobile code called infoatoms that contain information profiles and preferences that may be of use to data miners. These infoatoms combine with those of other individuals to form information crystals. In these crystals, the infoatoms interact, using zero-knowledge protocols to determine how many of their characteristics match. If enough characteristics match, the infoatoms turn on and reveal an aggregate picture of the set. The idea here is that individuals could sell information about themselves while maintaining some privacy. The information they reveal is useful to the data miner, but still allows the individual to hide amongst others with similar properties.

An example of how the system might work is illustrated in Figure 2. First, a data miner creates an infoatom seed that represents his query. For example, he may be interested in males with certain allergies. Then he participates in an anonymous financial transaction to get a set of infoatoms. The infoatoms that match the query and have sufficient similar infoatoms around them become activated and bind into a crystal. Finally, this crystal produces an aggregate report.

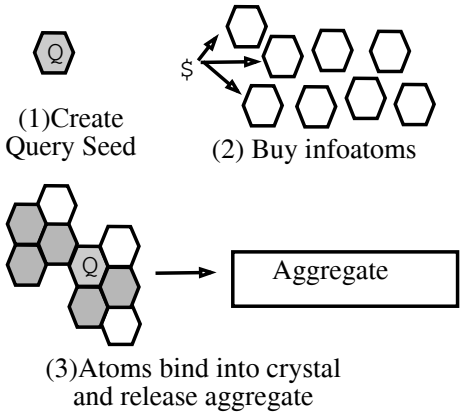

Figure 2: Querying [1]

5.1 Challenges in Implementing Information Crystals

There are a number of technical challenges that need to be overcome in order for the decentralized market for secrets to succeed. One issue with the information crystal approach is that the data miner can create an arbitrary number of false-name infoatoms and combine them with a single unknown infoatom in order to find out information about the unknown one. Since he knows the aggregate of the $n-1$ known atoms, all differences between that profile and the one emitted by the n atoms are a direct result of characteristics of the unknown infoatom. As a result the characteristics of the unknown infoatom can be inferred. In the anonymity literature, this is known as the $n-1$ attack. This attack can be somewhat mitigated by making the individual infoatoms small and uninteresting in and of themselves and making it difficult to determine which infoatoms would be interesting to attack in this manner. However, this attack should be addressed before such a system is implemented.

Another challenge is ensuring that individuals are honest about their information. It might be possible to address this problem by having profile properties certified by a trusted third party. This might also address the problem of false infoatoms created for the $n-1$ attack (though not valid but known infoatoms created for this purpose). This entails revealing this information to such a third party along with enough personally identifiable information to verify it to the third party. If this is not done carefully, the third party could become a centralized repository of personal information, just what this decentralized approach is trying to avoid.

The information crystals proposal requires secure mobile agents with obfuscated code. This is a difficult technical challenge. While there is some theoretical work that suggests that some functions may be obfuscated in order to produce secure mobile agents, [4] there is also a proof that in the general case obfuscation is impossible [9]. In addition, translating such a theoretical construct into a system which needs to run on an actual machine will be a challenge. Physical machines have open architectures and instructions that can be spied upon with a virtual machine.

In contrast to the National Information Market, these decentralized mechanisms assume that whenever any information is revealed to any agent the ability to extract additional revenue from that information is lost [20]. This avoids the need for a central audit trail, but creates perhaps the most difficult challenges. Currently, personal information is disclosed in the course of daily life. If we were given property rights to our information, they would be void almost immediately. In order for this system to have any meaning people must be able to release information in a minimal way without accompanying information. Ideally, you would want a strong infrastructure that built in privacy and anonymity. Information could be revealed to data miners in aggregate so that individuals could get the most out of their information profile.

So what is required to create this infrastructure for privacy? Not much, it would seem, if you read the cryptography literature.

> "Thus, cryptographic researchers might wish to believe that user privacy in e-commerce and content distribution is a solved problem. You pay for content or services with anonymous electronic cash. You connect to content or service providers via an anonymizing mixnet. You authenticate yourself with anonymous credential schemes or zero-knowledge identification protocols. You download content via private information retrieval or oblivious transfer. You use secure function evaluation when interacting with services that require some information [11]."

This quote sounds remarkably similar to statements in the "A Market for Secrets" paper about how their system would be realized [1]. However, it comes from a paper discussing barriers to these technologies [11]. Many such papers exist [11, 2, 19, 10] because despite intense research, analysis and in some cases commercial development these technologies are not in widespread use today. It is often postulated that this failure of adoption is due to social and economic factors, not technical ones. Some claim it is due to patent disputes (for digital cash, onion routing), others to high switching costs.

Perhaps it is intended to perpetuate the same externality and situation of asymmetric power that precipitated the desire for an information market.

Anonymity systems require inefficiencies in computation, bandwidth and storage. They require that a large number of users participate in order to provide a set in which users can hide [2]. They complicate online interactions, making it much harder to build workable reputation mechanisms and schemes for accountability [3]. Large scale anonymity tends to make law enforcement nervous, no matter how useful it is for undercover work or whistle blowing. There are attacks that make anonymity systems vulnerable to powerful, well-funded adversaries. An anonymous communications system depends on routing traffic through intermediate nodes at least one of which must be trusted. Who will be running the anonymous infrastructure that makes this system work? Who will pay for it?

Since it is a public good, perhaps the best answer to this question is everyone. But is that everyone in the governmental sense or in the private individual sense?

When the cypherpunks list was founded in the 1980s, it seemed like the rosy pseudonymous future was right around the corner [8]. It has remained there ever since. It will have to materialize somehow, if decentralized information mechanisms are to succeed.

5.2 An Incomplete Solution

Even if all the obstacles discussed in the previous section were overcome, the decentralized market for secrets would still not solve all of the world's privacy problems. There will still be a need and desire to communicate private information that is necessarily linked to an individual's identity and unable to be anonymized in a meaningful way. The decentralized market is a useful way to encourage more information to be aggregated and anonymized, however, and a market that incorporates this approach can provide incentives to utilizing this anonymity and promoting privacy in society at large. The Oregon law took steps in this direction when it provided an exemption from the property clause when genetic information was used for anonymous research. By giving individuals property rights over their information and thereby creating liability for its unauthorized use and investing in an infrastructure for data to be used anonymously the government might effectively provide incentives for privacy.

6 Efficient Markets Through Aggregation

The key issue with giving individuals property rights over their private information is allowing those rights to be maintained in a meaningful way in our electronic society. One approach to doing this is to implement an anonymous or pseudonymous infrastructure over which people can interact and do business without revealing personally identifiable information. Another approach is come up with a mechanism by which inappropriate use of personal information can be prevented, or at least tracked and punished. There are many technical and social challenges to either approach.

We have discussed how people can control and be compensated for their personal information and that any such design needs a well-understood market structure to avoid ambiguity and the pitfalls of the Oregon law. Ideally, an efficient market would avoid the need to pass around massive amounts of information and maintain detailed bookkeeping in order to conduct business using personal information. While individuals should license their personal information rather than giving away their rights outright in many cases, bookkeeping realities dictate that this is not a complete solution. However, we can extend the market solution to provide for aggregation and anonymization of personal data. This could work similarly to the proposal in Section 5, where individuals are compensated for participating in aggregate data which is unlinkable to them as individuals and then lose conrol of that data.

It is important to realize that not all personal information is created equal. For some types of information or information needs, the data is easy to combine into an aggregate which will provide all the information needed by the firm. In these cases, the market should encourage this aggregation. However, in many cases aggregation is simply not possible and other forms of regulation need to be explored. It is also the case that all types of personal information have their own issues which need to be clearly and unambiguously dealt with for the market to function. For example, in the case of genetic privacy, it is important to determine how a blood relative can exercise their interest in the DNA of another individual. The nature of the information protected may also dictate which technological, economic and legal mechanisms are best able to enforce fair markets for that information.

What personal information should individuals own? What information can be reasonably aggregated? These are interesting questions which should be explored in further research.

7 Framework for Personal Information Markets

Despite the problems with aggregation detailed in the previous section, there are situations in which aggregated data would be as useful, or almost as useful as data linked to individuals. If there exists a trusted third party to do the aggregating, it is possible to implement this mechanism in the near future. Less trusting mechanisms, such as the proposed Information Crystals, pose more implementation difficulties and require more research. Nonetheless, the problem is likely solvable in some cases. Perhaps the greatest obstacle to aggregated data is lack of market incentives for it. Why would you want aggregated data if you could get it linked to individuals? The incentives could be in the form of regulation, or in the avoidance of liability.

Aggregation might be incentivized best within a larger privacy market. Such a market requires legal changes making privacy a property right, a structure in which information rights could be easily negotiated, and the means to enforce these contracts. If digital rights management technology should mature, and there are plenty of arguments why it shouldn't, enforcing privacy markets would be a natural application for it. If not, then penalties for misusing the personal information of others need to be high. Requiring secondary users of personal information to possess a license for that information would be one way to facilitate enforcement. Since the rules for using such information are already complex (companies are forced to retain certain types of personal information for lengths of time) this becomes an interesting automated negotiation problem: the system must be flexible enough to provide consumers with meaningful privacy yet simple enough to not cause firms undue liability and cost. However, these costs and liabilities could act as incentives for aggregating as much information as possible.

8 Conclusion

In the current climate, personal privacy is eroding at a cost to individuals. While industry and government may benefit from the vast amounts of information available to them, they suffer in intangible ways as they lose the trust of individuals. A market for private information may hold the solution to this problem as individuals will regain control of their information and government and industry will have a mechanism to obtain the information they need. Before this can happen, however, government and industry will have to relinquish these rights to individuals, which may prove challenging. More research is required to determine how to implement and deploy an

infrastructure that allows these rights to privacy to be maintained.

Today, personal information is often given in addition to or in lieu of payment for another service. For instance, a subscription news website may require certain information of subscribers. Such bundling of information often leads to reduced privacy as consumers do not have a choice in whether to reveal information if they want the service. A good market for private information would recognize this problem and present alternatives to forced bundling. A market won't solve the problem of people not valuing their privacy. If people want to sell their DNA for a Big Mac, this market will only facilitate the transaction.

9 Acknowledgments

Thanks to David Parkes, Hal Varian, Glenn Holloway, Geoff Goodell, Stuart Schechterand Roger Dingledine for helpful comments and suggestions. Thanks also to H.T. Kung and the Department of Homeland Security for funding our research.

References

[1] E. Adar and B. Huberman, *A market for secrets*, First Monday 6(8), August 6, 2001, url=http://www.firstmonday.org/issues/issue6_8/adar/.

[2] A. Aquisti, R.Dingledine and P.Syverson, *On the Economics of Anonymity*, Financial Cryptography, Jan. 2003.

[3] C. Avery and P.Resnick and R. Zeckhauser, *The Market for Evaluations*, American Economic Review 89(3), pp 565-584, 1999.

[4] C. Cachin *et al., One-Round Secure Computation and Secure Autonomous Mobile Agents*, In: *Proceedings of the 27th International Colloquium on Automata, Languages and Programming* (ICALP), LNCS 1853, 512-523, 2000.

[5] Center for Democracy and Technology, *Surveys Main Page*, http://www.cdt.org/privacy/guide/introduction/surveyinfo.html, 2002.

[6] S.Cha, J.Young, *From P3P to Data Licenses*, Workshop on Privacy Enhancing Technologies, LNCS 2009, 2003.

[7] C. Collberg and C. Thomborson, *Watermarking, Tamper-Proofing, and Obfuscation: Tools for Software Protectionx*, IEEE Transactions on Software Engineering 28:8, 735-746, August 2002.

[8] cypherpunks, *The Cypherpunks Home Page*, http://www.csua.berkeley.edu/cypherpunks/Home.html.

[9] B.Barak, *et al,. On the (Im)possibility of Obfuscating Programs, Advances in Cryptology - CRYPTO 'O1*, Lecture Notes in Comp. Sci. 2139, pp.1-19, Santa Barbara, CA, August 19-23, 2001. Springer-Verlag.

[10] I.Goldberg, *Privacy-enhancing technologies for the Internet, II, Five years later*, Workshop on Privacy Enhancing Technologies, LNCS 2009, 2002.

[11] J. Feigenbaum *et al., Economic Barriers to the Deployement of Existing Privacy Technologies*, Workshop on Economics and Information Security, University of California, Berkeley, May 16-17, 2002, http://cl.cam.ac.uk/users/rja14/econws/23.pdf.

[12] geneforum.org, "Genetic Privacy: Oregon Genetic Privacy Statutes," http://www.geneforum.org/learnmore/gp/or_gps.cfm.

[13] H.Green, *et al., Our Four-Point Plan*, Business Week Online, http://businessweek.com/2000/00_12/b3673006.htm, March 2002

[14] A. Kiayias, M. Young, *Breaking and Repairing Asymmetric Pub lic-Key Traitor Tracing*, ACM DRM 2002.

[15] J.Kleinberg and C.Papadimitriou and P.Raghavan,*On the value of private information*, TARK: Theoretical Aspects of Reasoning about Knowledge, Vol. 8, 2001.

[16] K. Laudon, *Markets and Privacy*, CACM 39(9), 92-104, 1996.

[17] Microsoft, *Microsoft Next-Generation Secure Computing Base - Technical FAQ*, www.microsoft.com/TechNet/security/news/NGSCB.asp.

[18] D. Mulligan, A. Cavoukian, A. Schwartz, and M. Gurski, *P3P and Privacy: An Update for the Privacy Community*, http://www.cdt.org/privacy/pet/p3pprivacy.shtml

[19] A. Odlyzko, *Privacy, Economics and Price Discrimination on the Internet*, Workshop on Economics and Information Security, University of California, Berkeley, May 16-17, 2002, http://cl.cam.ac.uk/users/rja14/econws/52.txt.

[20] D. Parkes, *Challenge Problem: Agent-Mediated Decentralized Information Mechanisms*, In: *Agentcities: Challenges in Open Agent Envirnoments*, Burg et al. (eds.), Springer-Verlag, 2003.

[21] J. Santa and B. Speight, "Assuring Genetic Privacy in Oregon: The Report of the Genetic Research Advisory Committee," November 15, 2001.

[22] B. Schneier, "Secrets and Lies: Digital Security in a Networked World," John Wiley, New York, 2000.

[23] S. Shavell, *Principles of Economic Analysis of Law*, Chapter 7: Property Rights, http://econ.bu.edu/Weiss/Ec337/Shavell/bg7-1e.pdf

[24] Trusted Computing Group, www.trustedcomputinggroup.org.

[25] H. Varian, *Economic Aspects of Personal Privacy* In: *Privacy and Self-Regulation in the Information Age*, NTIA report, 1997, http://www.sims.berkeley.edu/ hal/Papers/privacy/

[26] T. Vila, R. Greenstadt, and D. Molnar, *Why We Can't Be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market*, Workshop on Economics and Information Security, 2003, http://www.cpppe.umd.edu/rhsmith3/