J O I N T C E N T E R
AEI-BROOKINGS JOINT CENTER FOR REGULATORY STUDIES

Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in The U.S. and The U.K.

Karim Jamal, Michael Maier, and Shyam Sunder

Working Paper 03-8
July 2003

The authors are Dr. Karim Jamal, Professor in the Department of Accounting & MIS at the University of Alberta; Michael Maier of the University of Iowa; and Dr. Shyam Sunder, James L. Frank Professor of Accounting, Economics and Finance at the Yale University School of Management. The authors gratefully acknowledge the assistance of John Dickhaut, Paul Healy and Joel Reidenberg. The views expressed in this paper reflect those of the authors and do not necessarily reflect those of the institutions with which they are affiliated.

J O I N T C E N T E R

In order to promote public understanding of the impact of regulations on consumers, business, and government, the American Enterprise Institute and the Brookings Institution established the AEI-Brookings Joint Center for Regulatory Studies. The Joint Center's primary purpose is to hold lawmakers and regulators more accountable by providing thoughtful, objective analysis of relevant laws and regulations. Over the past three decades, AEI and Brookings have generated an impressive body of research on regulation. The Joint Center builds on this solid foundation, evaluating the economic impact of laws and regulations and offering constructive suggestions for reforms to enhance productivity and welfare. The views expressed in Joint Center publications are those of the authors and do not necessarily reflect the views of the Joint Center.

All AEI-Brookings Joint Center publications can be found at www.aei-brookings.org

Executive Summary

Conventions as well as standards influence the practice of financial reporting. Financial reporting standards arise as legislated rules, enforced by the power of law. Conventions evolve over time through trial and practice, and are upheld by socioeconomic rewards and sanctions. Financial reporting in the second half of the twentieth century has been characterized by a preference for legislated standards, and a distinct lack of faith in its evolution as a body of social conventions. Evidence on whether this faith in standards over conventions is justified remains to be marshaled. We present data on privacy practices in e-commerce under the European Union's (EU's) formal regulatory regime prevailing in the United Kingdom (U.K.), and compare it to the data from a previous study of United States (U.S.) practices that evolved in the absence of government laws or enforcement. The codification by the EU law, and the enforcement by the U.K. government, improves neither the disclosure nor the practice of e-commerce privacy relative to the U.S. On the contrary, some evidence shows the unregulated practices in U.S. to be superior. Regulation in the U.K. also appears to stifle development of a market for web assurance services. Both U.S. and U.K. consumers continue to be vulnerable to a small number of e-commerce websites who spam their customers, ignoring the latter's expressed or implied preferences. We explore the implications of these results for understanding the merits of enforced standards and conventions in the domain of financial reporting.

Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in The U.S. and The U.K.

Karim Jamal, Michael Maier, and Shyam Sunder

1. Introduction

During the seven decades since the creation of the Securities and Exchange Commission (SEC), the concept of Generally Accepted Accounting Principals (GAAP) has gradually, but steadily, shifted from evolved social conventions toward legislated standards. Informal sanctions and reinforcements that sustain the evolution and effectiveness of social conventions have gradually been replaced by formal surveillance and penalties, backed by regulatory power to enforce the legislated standards. This fundamental shift in financial reporting regime, initiated in the United States (U.S.), has gradually spread to the rest of the world. The London-based International Accountings Standards Board (IASB, note the parallel nomenclature), which hopes to have its standards accepted around the globe, is the most notable example of the broad acceptance of the idea that legislated standards, backed by governmental power of enforcement, is a preferred financial reporting regime. Social conventions, backed by informal sanctions and market consequences, command little following at the turn of this century.

The widespread creation of institutions to write and enforce financial reporting standards has been accompanied by surprisingly little theoretical or empirical analysis of their possible merits relative to the evolutionary approach. Such analyses could be facilitated by the development of a framework that permits comparison of deliberately designed mechanisms or legislated standards on one hand, and evolved norms on the other. Hayek's ([1973], Chapter 1: Reason and Evolution) comparison of designed and evolved mechanisms is a good example. Coleman's [1990] analysis of social norms is another.

In this paper we present a direct comparison of empirical observations from a parallel field of e-commerce privacy, which is relevant to financial reporting. Jamal, Maier and Sunder (JMS, [2003]) documented the e-commerce privacy standards and practices in the U.S. where little government regulation or enforcement exists. The present study documents the e-commerce privacy practices and standards in the United

Kingdom (U.K.) where the Information Commission, a British government agency, currently enforces the privacy law of the European Union (EU).

A comparison of the U.S. and the U.K. practices reveals that the frequency of junk email received by those who register at e-commerce websites in the two countries is about the same. Only a small number of websites in the two countries violate the privacy of their customers by sharing personally identifiable information with third parties.[1] However, the unregulated disclosures of privacy policies in U.S. dominate the regulated disclosures in U.K. (from the consumer's point of view). This comparison raises important questions about the validity of the assumption that the standardized and enforced financial reporting regimes, which have gained significant currency around the world in recent years, dominate the evolutionary approach of generally accepted accounting principles.

The recent advent of e-commerce provides an opportunity to observe and compare privacy standards, disclosure, auditing and practices, with and without a regulatory regime in place. JMS [2003] documented the prevailing disclosure policies, the development of a market for independent web assurance services, and the privacy practices of 100 high traffic e-commerce websites in the U.S. during the second half of the year 2001. The key findings of JMS are: (1) Most e-commerce websites in the U.S. behave responsibly, provide good disclosure, and honor opt-in or opt-out choices of consumers, and (2) A small number of e-commerce websites account for an overwhelming proportion of abuses of consumer privacy.

In the present study, we use the JMS field experiment method and design to examine the disclosure and privacy practices of 56 high traffic websites in the U.K. which are formally regulated by the EU privacy law which have been incorporated into U.K. national privacy law (see Appendix A). The Information Commission (IC), monitors and enforces compliance with this law (see Appendix B for measures of compliance effort). We examine compliance with two key aspects of the law for which JMS have documented the corresponding U.S. practices: (1) The requirement to provide disclosure or notice of what consumer information is gathered and used by the website,

[1] We do not consider the security breaches which are unintentional, but have the same effect on violating the privacy of customers. For example, see Tedeschi [2003].

and (2) The consent requirement that consumers be provided with an option to control how their personal information is used by a website for secondary purposes.

Our results indicate that (1) Disclosure of privacy practices in the U.K. are no better, perhaps worse, than in the U.S. It is more difficult to find the privacy policy of a U.K. website, and compliance with the disclosure requirements of the U.K. privacy laws are generally quite poor. (2) Most websites in the U.K. honor the opt-out choices made by customers, just as in the U.S. Again there is no indication that U.K. websites behave better on average than their U.S. counterparts. (3) Most of the email received by the U.K. registrants comes from a single website that does not honor the opt-out option chosen by registrants, again similar to what happens in the U.S. (4) Even in the opt-in condition, most of the email comes from a single website, just as in the U.S. Overall we find no important differences between the average behavior of the British and American websites in this respect. Consumers in both regimes remain vulnerable to a small number of websites who misbehave. In the U.S., better companies have the opportunity to signal their good intentions to their visitors by investing a small amount of money in purchasing a web-seal from an independent provider such as TRUSTe or BBB Online. In the regulatory regime of the U.K., the market for web-seals does not exist. We outline the implications of the privacy findings for financial reporting in Section 5.

2. Regulation of Privacy Practices in the U.S. and U.K

The concept of privacy is deemed to be central to the development of an autonomous self and hence an important facet of individual liberty (DeCew [1999]). Until recently, privacy rights focused on the intimate details of one's life, such as the right to be silent about one's sexual preference, and the right to abortion. In addition, there was a general concern about providing government or other institutional authorities with too much information. There was less concern with privacy in business (DeCew [1999]).

That began to change with the rise of drug use in the general population in the 1960's and the1970's as business firms began to test prospective, even current, employees for drug use. More recently, electronic surveillance of the behavior of employees, and employer access to employees' genetic and medical records has raised

new privacy concerns relating to business (Kupfer, [1993], Brockett and Tankersley, [1997]).

With the Internet and the development of e-commerce, privacy issues became more complicated as a result of the new technology. New e-commerce technology has substantially increased the ability of online merchants to collect, monitor, target, profile and even sell personal information about customers to third parties (JMS [2003]). The intrusiveness of telemarketing activity and spam has raised the profile of privacy issues involving business.

In response to broad societal concerns about privacy, the Organization for Economic Cooperation and Development (OECD), the U.S. government, and the EU began extensive discussions in the 1970s about developing a regulatory framework for privacy. These discussions were guided by five privacy principles enumerated by the OECD [1980]: (1) Notice/Awareness: Participants should receive notice of an entity's information practices before they divulge any personal information. (2) Choice/Consent: Participants should be given options as to the uses of any personal information collected from them, especially for secondary uses that are unrelated to complete the original transaction (e.g., sale of information to third parties). (3) Access /Participation: A participant should have access to the information recorded about him and be able to modify any information that is deemed incorrect. (4) Integrity/Security: Collectors must take reasonable steps to ensure data integrity, convert it into anonymous form before using it for secondary purposes and destroy untimely data. (5) Enforcement/Redress: There must be a mechanism in place to enforce the privacy policies.

The EU decided to adopt a formal (legal) regulatory framework for the protection of privacy. In 1995 the EU parliament formalized the EU privacy law by passing the European Directive on Data Protection (EU Directive 95/46/EC). The Directive adopted the abovementioned five principles, and required the member countries to bring their national laws into compliance.[2] The Directive stipulated that personal data must be processed fairly and lawfully and only collected for a specified, explicit, and legitimate purpose. The use of data for any secondary purposes beyond the stated purposes is prohibited. Data cannot be kept any longer than needed to serve the stated purpose, and the data can only be collected if the person has given his or her consent. There is some

[2] These laws apply to all data collected on-line and off-line.

discretion available to each member country to define what "consent" means. Some countries, such as France, require consent to be obtained explicitly ("opt-in"), whereas the U.K. has a more permissive definition which allows consent to be implied as long as consumers are provided with an opportunity to opt-out of the use of their personal data for secondary purposes. The European Directive also requires each member government to create an independent government body to monitor the development, implementation and enforcement of national data protection law. Given that the U.S. has no law covering most websites, it is generally considered that, with respect to privacy laws, the EU has much stricter (and legally binding) standards and enforcement thereof than the U.S. does.

Data protection in the U.K. is regulated by the Data Protection Act (DPA) of 1984, which was significantly amended in 1998 for compliance with the EU Privacy Directive (Reidenberg and Schwartz [1998]). The Information Commission (IC), a U.K. government agency, is responsible for the monitoring and enforcement required by the EU directive. All entities collecting personal data must register with the Commission. The Commission has the statutory power to monitor compliance with the DPA, and can serve "enforcement notices" that direct a registered person to take specific steps to comply with the Act. The Commission can also cancel registration, prohibit overseas transfer of data, and can initiate prosecution of violators of the Act. Failure to register is subject to prosecution. Administrative decisions of the Commission, especially the enforcement notices, can be appealed to an independent Data Protection Tribunal. The budget of the IC more than doubled from £3,661,690 in fiscal year 1997-98 to £8,244,982 in 2001-02. Enforcement activities of the Information Commissioner are summarized in Appendix B. During the five-year period from 1997-2002, the IC filed 331 court cases and obtained 277 convictions for violation of the privacy law. Precedents established by the Data Protection Tribunal require that privacy notices be displayed in large, easy to read size in a prominent location, at the point where personal information is first collected. Reidenberg and Schwartz [1998] provide a detailed discussion of the EU privacy law and a comparison of national privacy laws of Belgium, France, Germany, and the U.K.

1995 was a watershed year—the EU passed its Privacy Directive and the U.S. did not pass a general privacy law. TRUSTe was formed in 1996 as a non-profit organization to promote better privacy practices and many U.S. websites voluntarily display a

TRUSTe web-seal to signal their compliance with the privacy standards formulated by TRUSTe. The Federal Trade Commission (FTC) started holding workshops in 1995 to discuss and promote good privacy practices. The FTC also tried to push e-commerce websites to improve their privacy practices by conducting studies (which combined a review of privacy policies and surveys) in 1998, 1999 and 2000. Each FTC study showed improvement in the actual practices of U.S. websites (FTC 2000). Congress has not passed any general privacy legislation to date, although several anti-spam laws are in the legislative process in mid-2003.

As of mid 2003, in the U.S., there is virtually no government regulation of privacy, and no legal requirement to disclose privacy policies in e-commerce or on the Internet. Once a person discloses information in the process of registering or transacting at a site, there are no legal constraints on what can be done with that personal information so long as no fraudulent actions are involved. There is no requirement that a site have a privacy policy, that consumers be informed about what data is being collected about them, and that consumers be provided with an option to give or deny their consent to secondary uses of the data gathered. In addition, there are no legally mandated audit procedures, nor are the e-commerce sites required by law to have their privacy policies certified by independent auditors[3].

3. Research Method and Results For Notice/Awareness Study

We gathered data from 56 high traffic websites in the U.K. by repeating the procedure used in the JMS [2003] study: first we obtained the addresses of high traffic websites from Jupiter Media Metrix (www.mediametrix.com), who monitors web usage and provides research and consulting services for online advertising. For countries other than the U.S., Media Metrix issues monthly reports of the top 15 active websites based on user traffic. We reviewed the top 15 reports from April 1999 – April 2002. This resulted in the identification of 28 websites that had been listed at least once in the top 15 rating report. We then picked firms in the U.K. Financial Times Index and looked for their websites. An additional 28 websites were identified where consumers could register or

[3] There are two exceptions to the lack of U.S. regulation of privacy- the health care industry and the financial services industry are governed by the Health Insurance Portability and Accountability Act (HIPAA - 1996) and the Gramm-Leach-Bliley Act (GLBA- 1999) respectively.

engage in transactions. A total of 56 high traffic websites in the U.K. were identified during the summer of 2002.

We programmed a web crawler to visit these sites and to record the use of their own, as well as any third party cookies. We also obtained an electronic copy of the privacy policies of these websites and looked for disclosure about cookie usage and the use of third party cookies. Our crawler visited each of the 56 websites five times during the week of June 4 -11, 2002. Some websites in the U.K. do not display a privacy policy until the consumer actually registers or initiates a transaction. We attempted to register or initiate a transaction during June 11-20 in order to identify the use of cookies. During the same period (May 27- June 12, 2002), a research assistant (who did not know the results generated by the web crawler) downloaded and date stamped the privacy policy of each website. The data collected using the crawler and by manual review of the privacy policies was combined in a spreadsheet for the analysis given below.

3.1 Disclosure (Notice/Awareness) Results

The results of the disclosure of privacy policies of the 56 high traffic U.K. websites are presented in Table 1 (alongside, for ease of comparison, the results from 100 high traffic U.S. websites reported by JMS). In the U.S., JMS report that 34 websites had paid for a privacy assurance web-seal from an independent party (30 TRUSTe, 2 BBB Online, and 2 had both TRUSTe and BBB Online). None of the websites in the U.K. displayed a web-seal. One consequence of a legislated standards approach to privacy appears to be the elimination, or preclusion, of a market for private web assurance. Since the law requires a disclosure of privacy policies but not privacy audit, there is no market for privacy assurance seals in the U.K. The privacy disclosure law appears to have eliminated the incentives for the websites to use web-seals as signals of their good privacy practices to consumers.

In the U.S., JMS reported that it was easy to locate the privacy policies of virtually all (97 percent) of the websites in the sample. In most cases, it could be located from the home page. In the U.K., we found it difficult to locate privacy policies on websites. The U.K. law requires the privacy policy to be provided before any personal data is collected. We therefore looked for the policy at the main home page, the registration page, and the page where personal information was entered. Our search

succeeded in only 77 percent of the websites in our sample. This suggests low compliance with the legal requirement to provide a privacy policy, and the precedents set by the Data Protection Tribunal requiring privacy policies to be prominent, easy to read, and provided before personal information is collected. Perhaps U.S. websites view the disclosure of privacy policies as an instrument of their marketing strategy to attract consumers, and make it easy to find this policy. U.K. websites, on the other hand, appear to view privacy disclosure as a matter of barely complying with the law, and make it quite difficult to find their statements of policy.

In the U.S., JMS [2003] reported that all 34 of the privacy seal websites, and 64 of the remaining 66 non-seal websites, used cookies, for an overall 98 percent cookie usage. The disclosure of cookie usage was also high, with all 34 privacy seal websites and 55 of the remaining 64 websites (overall 91 percent) disclosing their cookie usage. In the U.K. the rate of cookie usage was lower, with only 88 percent (49 out of 56 websites) using cookies to monitor consumers ($p<0.01$). The disclosure rate of cookie usage in the U.K. was also lower, with only 80 percent (39 out of 49) of the websites who use cookies disclosing their use thereof ($p<0.05$). Relative to the U.S., the formal legal codification of cookie disclosure requirements appears not to have improved disclosures in the U.K.

In the U.S., JMS [2003] report that third parties placed cookies on visitor hard drives in 31 (91 percent) of the websites with seals, and 48 (73 percent) of the websites without a seal, for an overall third party cookie usage rate of 79 percent. Thirty websites with a seal (97 percent) disclosed the presence of these third-party cookies on their site. Thirty of the 48 websites without a seal who were placing third party cookies (63 percent) disclosed the presence of third parties, for an overall third party cookie disclosure rate of 76 percent. In the U.K. websites were much less likely to allow third parties to use cookies to monitor customer behavior with only 50 percent of websites (28 out of 56) allowing third parties to place cookies from their site ($p<0.000$). In the U.K., 27 out of 28 of these websites (96 percent) disclosed the presence of third party cookies on their site. This is comparable to the 97 percent disclosure rate of the sites with a web-seal in the U.S., and better than the average U.S. disclosure rate of 76 percent ($p<0.01$).

For the remaining items in Table 1 (more explanation about cookies, third party cookies, and especially how data is used for secondary purposes), the disclosure rates in the U.K. are all lower than the disclosure rates reported by JMS [2003] for U.S. websites

($p<0.01$). Overall, it is clear that the privacy disclosures of the U.K. websites are no better than the privacy disclosures in the U.S. The rates of non-compliance with the requirements of the U.K. law are substantial; and only the third party cookie disclosure rates (96 percent) indicate a high level of compliance.

4. Research Method and Results For Choice/Consent Study

According to choice/consent, the second of the five OECD privacy principles, participants should be given an option to restrict the use of any personal information collected from them, especially for secondary uses unrelated to the processing of the transaction at hand. Websites use two primary options to let users control the use of their personal information. Opt-out, the most common option, allows users to explicitly restrict the website from transferring their data to any third party not involved directly in processing the transaction for which the data were collected. A second option is to require an explicit "opt-in" from the consumer, which expressly permits the website to use the data for secondary purposes such as internal and possibly external marketing. The opportunity to opt-out (or opt-in) is widely regarded as a key choice mechanism and U.K. law requires that at least an opt-out option should be provided whenever personal data is collected.[4] The evidence gathered is summarized next.

We examined the effectiveness of the "opt-out" feature of websites by registering on the same 56 high-traffic websites used to test disclosure policies in Section 3 above. We used the JMS [2003] procedure to monitor compliance of websites with privacy standards. We set up a private U.K. domain name, created 112 identities (name, U.K. email address, U.K. based postal address, U.K. phone number with voice mail, and credit card number). These email accounts were secure in our private domain and could not be accessed by robots or telemarketers looking for public directories of email addresses. Each of the 56 pairs of identities could be uniquely traced to one of the 56 website where we used it for registration.

We registered twice on each of the 56 websites under two different identities. Following the JMS procedure, we conducted one transaction (e.g., sent a greeting or email, or set up a portfolio) at the time of registration. We used the first set of 56

identities to register on each of the 56 websites and did not place any restriction on having our data shared with others, that is, we "opted-in" to receive messages and materials, such as magazines, relevant to our simulated identity. The second set of identities was used to register again on the same sites, where we "opted-out" immediately from having our information shared with both internal and any external parties. In the second registration we did not accept any free offers. Note that our registration procedure enabled us to uniquely identify the 112 sources (opt-in and opt-out registrations at 56 sites) of any incoming email because the name and email address used in each registration were different. All registrations were completed between September 2-8, 2002.

4.1 Results: Choice/ Consent

We attempted to register on all 56 websites used in the disclosure part of the study. Of the 56 websites, 40 websites allowed us to opt-in, and only 25 websites allowed us to opt-out. Table 2 shows the weekly means (standard deviations) of the number of email messages received over the 26-week period following the registrations in the U.S. (as reported by JMS) and our data from the U.K. The top part of Figure 1 shows a chart of the weekly mean frequency of email messages from the U.S. opt-in (gray square), and the U.K. opt-in (black square). The two middle lines in Figure 1 show the U.S. opt-in excluding the highest volume website (gray triangle), and the U.K. opt-in excluding the highest volume website (black triangle). The bottom two lines in Figure 1 show the U.S. opt-out (gray circle), and the U.K. opt-out (black circle) website registrations in both the U.S. and the U.K. Most websites generated one confirmation message immediately following the registration.

JMS reported receiving few messages from opt-out registrations in the U.S.; the mean was only 0.45 messages per week. JMS also reported that most of the messages in the opt-out condition were generated by a handful of websites; one site generated 48 percent of all email messages and the top five sites accounted for 92 percent of all email received. Excluding these outliers, the mean number of weekly email messages was close to 0. In the present study of U.K. opt-out registrants, we received 468 commercial

[4] An opt-in system protects privacy better than opt-out does, because each option is the default for the other. Most users end up with the default option through their failure to make an explicit choice between opt-in and opt-out.

email messages over the 26-week data collection period, for an average of 0.75 messages per week from opt-out registrations. The U.K. data are also largely driven by a single website that accounted for 93 percent of all the messages from opt-out websites. If we exclude this outlier, the mean number of weekly messages to opt-out registrants in the U.K. is also close to 0. The difference between the average number of messages received from opt-out registrations in the U.S. and the U.K. is not statistically significant. It does not matter if we look at all the data (GLM, $F[1,65]=0.28$, $p=0.6007$), or exclude the one extreme observation from the U.K. data, and five extreme observations from the U.S. data (GLM,$F[1,59]=1.15$, $p<0.288$)[5].

For opt-in registrants in the U.S., JMS reported receiving significantly more email with a mean of 8.44 emails per week. As in the opt-out condition, JMS reported that one outlier generated 56% of all the opt-in messages received. After excluding this outlier, the mean level of email was 3.81 per week in the U.S. (still significantly more than the mean level of email received by opt-out registrants at $p<0.000$). In the present study, the U.K. opt-in registrants received 9,563 email messages over the 26-week period of this study for an average of 9.20 messages per registration per week. This is 12 times the average volume of email messages received by the opt-out registrants. Paired sample t-test yields a mean difference of 8.45 ($t = 14.74$, 25 df, $p <0.000$). This result in the U.K. of opt-in receiving more email than opt-out registrants is also consistent with the data reported by JMS [2003] for the U.S.

Beginning with an average of about 2 email messages per week in the first week (see Figure 1, black square legend) the average level of email from U.K. websites rose steadily to about 14 per week in week 26. Like the opt-out results described earlier, the U.K. opt-in results were also driven in large part by a single website. Some 66 percent of all opt-in messages (a total of 6,342 messages over 26 weeks for an average of 244 per week) came from this single registration. Excluding the messages from this one outlier (black triangle legend), the email volume from the U.K. based opt-in sites gradually rises from about 2 per week to about 4.5 per week by the end of the 26-week period. This is more than 4 times the email volume for the opt-out registrants. Excluding the outlier data from the opt-in sample, the opt-in messages (mean of 3.18 email messages per week)

[5] We obtain the same pattern of results even if we eliminate only 3 outliers from the U.S. opt-out data $F(1,61) = 0.18$, $p=0.6691$.

continues to be significantly more than the opt-out messages (mean difference = 2.42, t=27.55, 25 df, p< 0.000). This pattern of results also replicates the U.S. data reported by JMS [2003]. There is no significant difference between the opt-in email level in the U.S. and the U.K. for both total email received (GLM, F[1,107]= 0.01, p=0.9231) as well as after excluding one outlier from each of the U.K. and the U.S. opt-in data (GLM, F[1,105]=0.14, p=0.7063).

5. Implications For Financial Reporting

As outlined in Section 2, the U.K. (and the EU) chose to protect the privacy of their citizens by legislating standards to be monitored and enforced under the powers of government. The U.S., on the other hand, chose, by deliberation or default, to allow the privacy policies in e-commerce to evolve as norms or conventions of e-commerce without legislated standards or a punitive enforcement mechanism.

Our comparative study of the performance of these two regimes covers two dimensions of privacy. On the choice/consent dimension (i.e., participants controlling any secondary uses of their personal information) we find that the performance of the two regimes, as measured by the number of email messages sent to those who do and do not give consent to receive such messages, is almost identical. With only a few exceptions, most e-commerce sites honor the choice exercised by the registrants. Under both regimes, a few websites flood their registrants with commercial email messages, disregarding the latters's wishes. Registrants who indicate their willingness to receive commercial email messages receive a comparable level of message traffic under both regimes.

On the notice/awareness dimension (i.e., participants receiving timely notice of an entity's information and privacy policies), by most measures, the standards and enforcement regime of the U.K. is no better than the evolutionary regime of the U.S., and is inferior on some dimensions. For example, in spite of the privacy law and enforcement mechanism, fewer U.K. websites post their privacy policies. It is more difficult to find the privacy policy statement on U.K. websites even when they are posted. These websites are less likely to disclose the use of cookies and how the data gathered is used for secondary internal, and external marketing purposes.

In the absence of legislated standards and their government enforcement, a market for web assurance services, including privacy assurance, has arisen in the U.S. About a

third of the U.S. websites in the JMS [2003] sample chose to pay a small fee to the sellers of such services (e.g., TRUSTe and BBB Online) and had them certify that: (1) The website policies conformed to the privately developed standards of the assurance service provider, and (2) The website practices conformed to the website's stated policies. The U.S. websites that displayed the service providers' assurance seals performed at least as well as, and on average better than, the U.K. websites in protecting the privacy of their users.

The legislation and enforcement mechanisms in the U.K. and the EU were set up on the assumption that they will help improve privacy on the Internet. Our comparative study of the U.K. and the U.S. reveals that privacy has fared no better, and perhaps worse, in the U.K. than in the unregulated U.S. environment. How could we explain this apparent disparity?

5.1 Statutory Law and Social Conventions

Codified standards with formal enforcement are concrete and salient. Extant standards are published, easily disseminated, specified formally with some precision, and can be analyzed and discussed.[6] They come into existence at a specific time, through a known and understood institutional process that may allow the participation of the constituents. When the environment changes, or the standards are no longer perceived to induce the desired patterns of behavior, there is a systematic process available to formulate changes and submit them to a well-specified process for possible promulgation.

A transparent institutional mechanism for setting and modifying standards holds a natural appeal in a democratic polity. Following accidents and scandals, "the rules were not clear" is a popular defense for scoundrels and managers who have not adopted good data handling practices. Codification of standards—let us make the rules clear to all—is a frequently chosen response to calm the political waters. Formal written standards also appeal to our sense of good housekeeping.

Social conventions and norms are less well defined, vary in time and space, and require an extended socialization process to learn and understand (Coleman [1990]). Conventions carry a penumbra of uncertainty about the edges; there is substantial but incomplete overlap among the beliefs of the individual members of a group about its

[6] See Fuller [1964] and Dworkin [1986] for discussion of natural law theory.

norms. Even with a unique definition in time or place, norms evolve in small, almost imperceptible steps by processes that are not well understood. The evolution of norms is decentralized in the extreme, and even experts find it difficult to predict their direction. While the evolutionary process is not opaque, the lack of definition and our lesser understanding of how norms develop and evolve make them less transparent. When a scandal occurs, existing institutions face a legitimacy crisis, since the scandal itself mocks the claims of expertise and efficiency required to legitimize existing institutions. It is hardly surprising, then, that during periods of crises, political or bureaucratic decision makers feel pressure to write new standards rather than continue to rely on existing (recently discredited) norms and business practices.

Formal standards require formal enforcement mechanisms to be effective. Government departments, courts and regulatory agencies, industry associations and private sector organizations in national and international domains monitor the implementation of various kinds of standards, and furnish procedures to impose penalties on violators. Formal enforcement of informal social conventions is difficult. However, social relationships among business participants makes it possible to create a "word-of-mouth" mechanism where feedback and reputation can be enhanced (or damaged) rapidly and a sense of community can be formed among interested parties. New Internet technologies make it possible for people to significantly expand these social networks (Dellarocas [2003]).

As we have seen from the data presented in this paper from two jurisdictions, the opt-out regime works surprisingly well and almost identically in both. Exercising the opt-out option enables users to avoid virtually all the junk email.[7] A few sites promise, but fail to honor the opt-out provision. Formal regulation coupled with government enforcement appears to have little effect on the average behavior of websites. Moreover, formal regulation does not appear to provide protection from the extreme behavior of a few websites. This is consistent with what we observe in financial reporting: Enron, WorldCom and other companies were mired in accounting scandals in the most extensively regulated financial reporting environment in the world.

[7] Note that registration and transactions at e-commerce sites are not the only source of email addresses for bulk junk mailers. Email address lists for spammers are compiled from many other sources, such as websites which list personal addresses, and from legitimate email.

With all its apparent advantages of clarity, explicitness, and the power of enforcement, the standards approach also suffers from several disadvantages relative to the evolutionary or social convention approach to regulation. In the following section we examine these issues in the context of financial reporting, although much of what we have to say is applicable to other fields.

5.2 Standards vs. General Acceptance in Financial Reporting

When the U.S. Congress created the Securities and Exchange Commission (SEC), and gave it the legal authority to regulate financial reporting in 1933, financial reporting practice was governed largely by convention. The first three decades of regulation were devoted largely to codifying these conventions into GAAP. These seven decades have seen a gradual, but inexorable, shift from convention or social norm approach to legally enforceable standards. The shift is also reflected in the increasingly assertive nomenclature of the three private sector organizations entrusted with the task of writing accounting rules and their publications: The committee on Accounting Procedure's Accounting Research Bulletins (1948-59), the Accounting Principles Board's Opinions (1959-73), and the FASB's Financial Accounting Standards (1973 to present).

By the turn of the century, the social norm or convention approach of the earlier years is almost forgotten. The U.S., followed by much of the rest of the world, now favors a more formal legislated standards (with legal enforcement) model for financial reporting. Yet, the evidence that formal standards do any better than social norms of financial reporting remains elusive. To the extent the empirical evidence reported in this study on e-commerce privacy is relevant to financial reporting it goes the other way.

In the following paragraphs, we consider four possible reasons for why formal legal standards with state enforcement, with their apparent advantages, may not be as effective as social norms in financial reporting. We label them as the information, design, gaming and signaling problems.

The Information Problem

The most difficult problem any rule maker faces is the identification of a good rule. Rules affect many members of society in diverse ways. The direct effect of the rules

on people depends on their individual circumstances that the rule maker knows little about. Rules are designed in the hope that they will change or constrain, the behavior of at least some people. This change also depends on the individual circumstances not known to the rule maker. The changes in the behavior of individuals interact in complex ways to generate aggregate consequences that are often difficult to anticipate. The rule maker may try to ameliorate this informational disadvantage by soliciting information from the parties potentially affected by its actions. Unfortunately, these parties have little incentives to report truthfully, and their strategic responses only muddy the waters (see Sunder [1997], Chapter 11), and create the gaming problem discussed below, often forcing the rule maker to deal with unintended consequences of their rules.

The evolution of social conventions proceeds in fits and starts, with little guarantee of progress. Each small or large change in conventions is induced by and induces changes in individual behavior, moving the social system to a new, albeit temporary, expectations equilibrium (see Sunder [2002]). People get the chance to experience the consequences of each change, and adjust their behavior to the new circumstances. Information in possession of the individuals that rule makers cannot capture for their decision-making gets aggregated into these outcomes through market and other social processes (see Hayek [1945]). For this reason the evolved social norms often incorporate more information than the rules made by corporate entities, such as legislatures and boards.

The Design Problem

The Corporate entities for setting standards need a structure, people, and resources. All three force compromises in the design of the entity. Legislative structures emphasize representativeness, judicial structures emphasize impartiality, while bureaucratic structures value rules of procedure above all. It is not possible to attain perfect representativeness, impartiality, and consistency of procedure all at once. Finding the people to operate the rule-making system runs into parallel problems. The best experts may not be representative or impartial, and they may be inclined to use their judgment over pre-defined procedures. Representative bodies may lack expertise in the substance of the matter, and do not place impartiality high on their agenda, and so on. Finally, those who pay for the cost of developing standards seek their own agendas

through their influence over the finances of the standard-setting entity. Such inevitable compromises "corrupt" the standard-setting bodies. The gradual evolution of social conventions can be said to be free of these weaknesses of corporate entities because such entities do not play a major role in the process.

The Gaming Problem

The difficulty posed by the information problem discussed above is compounded by the dynamics between rules and the behavior the rules are intended to influence. Each standard alters the decision environments of the relevant individuals, and at least potentially alters their decisions. Standards also induce the individuals to search for new alternatives, or create opportunities that may not have existed earlier. The rule makers, with limited information, cannot anticipate all such changes, and the rules often lead to unintended consequences in the form of individual behavior and their social outcomes. For example, Tan and Jamal [2003] found that changing discretion in accounting rules has an unintended effect of changing the "real" operating decisions of managers. Any adjustment of the rules to such outcomes sets up yet another cycle of adjustments and changes. Individuals can adjust faster than the rule makers can. It is difficult to make sure that this action-reaction sequence converges to a rule and pattern of behavior, which are in equilibrium with each other. Informality and the flexibility of social norms have a better chance of effectively dealing with this gaming problem through evolution stretched over a long period of time.

The Signaling Problem

A formal standards approach to financial reporting favors narrowing the range of options available to the reporting entity. Many believe that a narrower set of choices available to the accounting entity in how to report a given event or transaction promotes comparability and consistency, and enhances the value of financial statements. Valid as this argument might be, it also ignores the signaling value of the choices made by the reporting entity. In making a choice from a given set of alternatives, the entity cannot help but reveal information it holds privately about its preferences and expectations. Managers of the entity reveal their privately held information, in part, through the financial reporting methods they choose (Levine [1996]). The use of aggressive reporting

methods gives valuable information to careful readers of the financial reports. Narrowing financial reporting choices through strict standards also eliminates the ability of managers to transmit information through their choice of financial reporting methods.

6. Conclusion

One consequence of a legislated approach to setting e-commerce privacy standards appears to be the elimination, or preclusion, of a market for private web assurance. Since the law in the U.K. specifies privacy disclosure requirements, and there is no legal requirement to purchase a privacy audit certificate, there is no market for privacy assurance seals. Contrary to its intent, the privacy disclosure law appears to have eliminated the incentives for the websites to use web-seals as signals of their good privacy practices to consumers.

In financial reporting, the legal requirement of independent audit of publicly held firms seems to serve as an obstacle to the efficient functioning of a market for audit services. If independent audit were not a legal requirement, firms with sufficient confidence in their accounts and in their prospects would spend the money to hire reputable independent auditors to convince their shareholders about their transparency and good prospects. Firms without such confidence will not find it worthwhile to hire auditors. Investors, presented with reports with and without auditor certificates will have to make their own risk assessments and price the securities accordingly. Without government regulation, a market for certification or audit services would develop analogous to the U.S. market for web services in e-commerce. JMS [2003] adduce evidence of a web certification market for privacy assurance, and DeWally and Ederington [2003] analyze the evolution and functioning of an audit certification service for online comic book auctions on eBay. Instead of allowing such a market to develop, the SEC requires all firms to have their reports audited, and tries to specify the standards by which the auditing must be carried out. The extensive regulation of audit practice has been accompanied by commoditization of the audit, and the widespread auditing scandals of recent years.

In the absence of mandated standards, U.S. websites tend to view the disclosure of privacy policies as an instrument of their marketing strategy to attract consumers.

Accordingly, they make it easy to find their statements of policy, and adhere to these policies reasonably closely. U.K. websites, on the other hand, appear to view privacy disclosure as merely a compliance matter; they appear to be, at the very least, indifferent to the consumer concerns about their privacy policies, and on average, make it more difficult than in U.S. for their customers to find their statements of policy.

Our conclusions from the comparison between U.S. and U.K. data should be moderated by several considerations. First, the data in the U.S. were gathered one year earlier. The U.S. disclosure data collection (July) and website registrations (August) were done by JMS in the summer of 2001, whereas our U.K. disclosure data collection (May/June) and website registrations (September) were done in the summer of 2002. It is possible that a shift in the e-commerce practices may have occurred during this interval, eroding the validity of the comparisons presented here.

Second, we are careful registrants who opt-out immediately upon registration and follow the JMS [2003] procedure of visiting only high traffic and reputable websites. It is possible that less careful registrants may get much larger volumes of unwanted (spam) email.

Third, there are many differences between the U.K. and the U.S., and between e-commerce privacy and financial reporting which require us to exercise caution in making analogies from one jurisdiction to another (Healy [2003]). Our study is not a perfectly controlled experiment, so an inferential leap must be made across these jurisdictional differences.

Law, auditors, reputation, business norms and practices, warranties, disclosure, and industry associations are competing trust creation mechanisms associated with markets. The value of each mechanism depends on the set of mechanisms available in a particular market. While each mechanism may be useful in isolation, the marginal value of some over others may be small. A large body of literature in psychology (Cook [2001]), sociology (Granovetter [1985]) and political science (Putnam [1993]) suggests that key trust creation mechanisms in society are personal relationships and social embeddedness of market participant's rather then legal rules and formal enforcement structures. Our results suggest that the value of legal regulation and enforcement may be

overestimated when the availability of alternative trust generation mechanisms is ignored in studies of accounting regulation. Future research can help us understand the incremental value of formal legal regulation and enforcement in situations where other trust creation mechanisms are available.

References

Brockett, P.L., AND S.E. Tankersley. "The Genetics Revolution, Economics, Ethics, And Insurance." *Journal of Business Ethics* 16 (1997): 1661-1676.

Coleman, J. *Foundations of Social Theory*. Harvard University Press, Cambridge, MA, 1990.

Cook, K.S. (Ed.) *Trust In Society.* Volume II in The Russell Sage Foundation Series on Trust. New York, NY: Russell Sage Foundation, 2001.

DeCew, J.W. *In Pursuit of Privacy: Law, Ethics and The Rise of Technology*. Cornell University Press, Ithaca, NY, 1990.

Dellarocas, C. "The Digitization of Word-of-Mouth: Promise and Challenges of Online Feedback Mechanisms." Working paper, MIT Sloan School of Management, Cambridge, MA, 1999.

DeWally, M., AND L. Ederington. "A Comparison of Reputation, Certification, Warranties, and Disclosure as Remedies for Information Asymmetries: Lessons From The On-line Comic Book Market." Working paper, University of Oklahoma, 2003.

Dworkin, R.M. *Law's Empire.* Harvard University Press, Cambridge, MA, 1986.

European Parliament. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on The Protection of Individuals With Regard to The Processing of Personal Data and on the Free Movement of Such Data.* O.J. L281 (Nov 23, 1995).

Federal Trade Commission (FTC) "Privacy Online: Fair Information Practices in the Electronic Marketplace." Washington, DC (May 25, 2000).

Fuller, L.L. *The Morality of Law*. Revised Edition. Yale University Press, New Haven, CT, 1964.

Granovetter, M. "Economic action, social structure, and embeddedness." *American Journal of Sociology* 91 (1985): 481-510.

Hayek, F.A. "The Uses of Knowledge in Society." *American Economic Review* 35 (September 1945), 519-30.

____. *Law, Legislation and Liberty.* Vol. I: Rules and Order. University of Chicago Press, Chicago, IL, 1973.

Healey, P. "Discussion of Privacy in E-Commerce: Development of Reporting Standards,

Disclosure and Assurance Services in an Unregulated Market." *Journal of Accounting Research* 41 (2), (May 2003): 311-315.

Jamal. K.; M. Maier; AND S. Sunder. "Privacy in E-Commerce: Development of Reporting Standards, Disclosure and Assurance Services in an Unregulated Market." *Journal of Accounting Research* 41 (2) (May 2003): 285-309.

Kupfer, J. "The Ethics of Screening in the Workplace." *Business Ethics Quarterly* 3 (1) (1993): 17-25.

Levine, C. "Conservatism, Contracts, and Information Revelation." PhD Dissertation, Carnegie Mellon University, 1996.

Organization for Economic Cooperation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* 1980. Available from http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM.

Putnam, R.D. *Making Democracy Work*. Princeton University Press. Princeton, NJ, 1993.

Reidenberg, J.R., AND P.M. Schwartz. *Online Services and Data Protection Law: Regulatory Responses*. Published by European Commission's Office of Official Publications, Euro-Op, (1998).

Sunder, S. *Theory of Accounting and Control*. Cincinnati, OH, Thomson Learning, 1997.

____. Management Controls, Expectations, Common Knowledge and Culture. *Journal of Management Accounting Research* 14 (2002): 173-187.

Tan, H.C., AND K. Jamal. "The Effect of Accounting Discretion on Income Smoothing and The Production-Investment Decisions of Managers." Working paper, University of Alberta, 2003.

Tedeschi, B. "F.T.C. Increases Focus on Privacy," *The New York Times* (June 30, 2003), Section C, Pg 5.

Table 1: Disclosure of Privacy Policies

Number	Privacy Practice	U.S. Websites With Privacy Seals (N=34)	U.S. Websites Without a Privacy Seal (N=66)	Total U.S. Websites (N=100)	U.K. Websites With EU Privacy Law (N=56)	Test of Equality of Proportions Z Value (p value)
1	Post a Privacy Policy	34 (100%)	63 (95%)	97 (97%)	43 (77%)	12.53 (p<0.000)
2	Privacy Policy is One Click Away	34 (100%)	61 (92%)	95 (95%)	39 (70%)	4.32 (p<0.000)
3	**Use Cookies to Track User Behavior**	**34 (100%)**	**64 (97%)**	**98 (98%)**	**49 (88%)**	2.6 (p<0.01**)**
4	Disclose Website is Using Cookies	34 (100%)	55 (86%)	89 (91%)	39 (80%)	1.87 (p<0.05)
5	Explain What Cookies Are	30 (88%)	42 (66%)	72 (74%)	37 (76%)	0.265 (p<0.40)ns
6	Explain How to Turn Off/ Decline Cookies	19 (56%)	23 (36%)	42 (43%)	25 (51%)	0.93 (p<0.18)ns
7	**Allow 3rd Parties to Use Cookies on Website**	**31 (91%)**	**48 (73%)**	**79 (79%)**	**28 (50%)**	3.76 (p<0.000)
8	Disclose Presence of 3rd Party Cookies on Website	30 (97%)	30 (63%)	60 (76%)	27 (96%)	2.32 (p<0.01)
9	Provide Link to Privacy Policy of 3rd Party	19 (61%)	20 (42%)	39 (49%)	4 (14%)	3.27 (p<0.001)
10	Disclose How Data are Used for Internal Transaction Processing	34 (100%)	63 (95%)	97 (97%)	43 (77%)	4.0 (p<0.000)
11	Disclose How Data are Used for Internal Marketing Purposes	34 (100%)	62 (94%)	96 (96%)	44 (79%)	3.4 (p<0.001)
12	Disclose How Data are Used for Outsourced Transaction Processing by a 3rd Party	28 (82%)	43 (65%)	71 (71%)	23 (41%)	3.66 (p<0.000)
13	Disclose How Data are Used for Marketing Purposes by 3rd Parties	34 (100%)	62 (94%)	96 (96%)	32 (57%)	6.09 (p<0.000)

In a field experiment, Jamal, Maier and Sunder (JMS [2003]) programmed a web crawler to repeatedly visit 100 selected high traffic websites in the U.S. during the week of July 23-29, 2001, and to record what cookies (and third party cookies) are used by these websites to monitor visitors to the websites. JMS then download the privacy policies of these 100 websites and record the number of websites who disclose their use of cookies (and third party cookies), as well as disclosures on how data collected from participants is used and shared internally and with external third parties. U.S. websites are classified into two groups: those that purchase an independent web assurance seal (n=34), and those who do not have a web-seal (n=66). We applied the JMS procedure during the period of May 27 -June 12, 2002 for 56 high traffic U.K. websites which are governed by EU privacy law. A U.K. government body monitors and enforces the privacy law in the U.K. None of the U.K. websites had a web-seal.

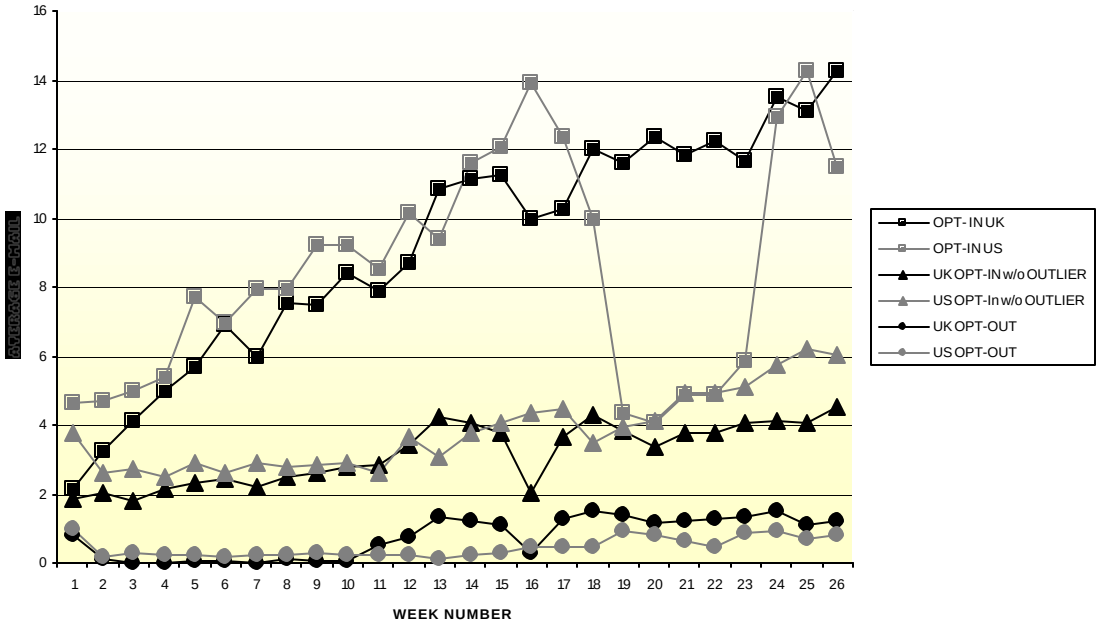
Table 2: Mean (Standard Deviation) Number of Email Messages Received For Opt-In and Opt-Out Website Registrations

Week	US Opt-In (n=69)	UK Opt-In (n=40)	US Opt-In w/o Outlier (n=68)	UK Opt-In w/o Outlier (n=39)	US Opt-Out (n=43)	UK Opt-Out (n=25)
	4.62	2.13	3.78	1.87	0.98	0.80
1	(8.73)	(2.59)	(5.24)	(2.07)	(0.91)	(0.71)
	4.71	3.25	2.63	2.03	0.19	0.12
2	(17.98)	(8.37)	(5.07)	(3.22)	(0.82)	(0.44)
	5.00	4.13	2.71	1.82	0.30	0.00
3	(19.77)	(14.88)	(5.29)	(3.04)	(0.89)	(0.00)
	5.41	4.98	2.51	2.15	0.21	0.00
4	(24.56)	(18.15)	(5.20)	(3.39)	(0.71)	(0.00)
	7.74	5.68	2.88	2.31	0.26	0.04
5	(40.66)	(21.54)	(5.10)	(3.24)	(1.09)	(0.20)
	6.96	6.90	2.62	2.41	0.19	0.04
6	(36.42)	(28.60)	(5.30)	(3.49)	(1.08)	(0.20)
	7.93	6.00	2.93	2.23	0.21	0.00
7	(41.98)	(24.06)	(6.07)	(3.28)	(0.97)	(0.00)
	7.96	7.55	2.79	2.51	0.23	0.12
8	(43.25)	(32.06)	(5.65)	(3.64)	(1.02)	(0.44)
	9.23	7.48	2.87	2.59	0.28	0.04
9	(53.2)	(31.15)	(5.96)	(4.00)	(1.10)	(0.20)
	9.20	8.43	2.90	2.77	0.26	0.08
10	(52.74)	(36.01)	(6.23)	(4.23)	(1.05)	(0.40)
	8.54	7.90	2.63	2.82	0.21	0.52
11	(49.34)	(32.33)	(5.46)	(3.68)	(0.97)	(2.40)
	10.13	8.68	3.68	3.44	0.26	0.76
12	(54.22)	(33.53)	(8.18)	(5.17)	(1.03)	(3.80)
	9.41	10.83	3.07	4.26	0.12	1.36
13	(53.05)	(42.18)	(6.92)	(7.38)	(0.45)	(5.99)
	11.59	11.15	3.78	4.08	0.23	1.24
14	(65.48)	(45.32)	(8.64)	(7.38)	(0.92)	(6.20)
	12.04	11.28	4.07	3.79	0.28	1.12
15	(66.87)	(47.76)	(9.45)	(6.60)	(1.10)	(5.60)
	13.94	9.98	4.32	2.05	0.49	0.28
16	(80.53)	(50.19)	(10.11)	(2.76)	(1.67)	(1.40)
	12.36	10.25	4.46	3.64	0.49	1.28
17	(66.72)	(42.45)	(11.84)	(7.52)	(2.04)	(6.40)
	10.00	11.98	3.49	4.28	0.47	1.48
18	(55.16)	(49.39)	(10.78)	(8.58)	(2.07)	(7.19)
	4.33	11.58	3.93	3.82	0.91	1.40
19	(14.27)	(49.68)	(13.97)	(8.03)	(4.46)	(7.00)
	4.04	12.35	4.10	3.38	0.79	1.16
20	(13.89)	(57.09)	(13.99)	(6.71)	(3.90)	(5.80)
	4.86	11.85	4.93	3.77	0.63	1.20
21	(17.18)	(51.59)	(17.30)	(7.12)	(2.95)	(6.00)
	4.87	12.23	4.93	3.79	0.44	1.28
22	(17.54)	(53.81)	(17.66)	(7.36)	(1.98)	(6.40)
	5.88	11.68	5.07	4.08	0.86	1.36
23	(20.48)	(48.66)	(19.48	(7.77)	(4.21)	(6.80)
	12.94	13.50	5.72	4.13	0.91	1.48
24	(63.64)	(59.85)	(21.43)	(8.39)	(4.94)	(7.40)
	14.28	13.13	6.22	4.05	0.70	1.12
25	(71.53)	(57.79)	(25.48)	(6.90)	(3.46)	(5.60)
	11.49	14.25	6.01	4.51	0.79	1.20
26	(51.76)	(62.04)	(24.84)	(7.61)	(4.30)	(6.00)
Average	8.44	9.20	3.81	3.18	0.45	0.75

In a field experiment, Jamal, Maier and Sunder (JMS [2003]) constructed 200 identities (name, address, email address) and attempt to register twice on each of 100 high traffic websites in the U.S. In the opt-in registrations (n=69), JMS allow the website to use their personal data for both internal marketing purposes, and to sell personal data to external third parties. In the opt-out registrations (n=43), JMS do not allow the website to use their

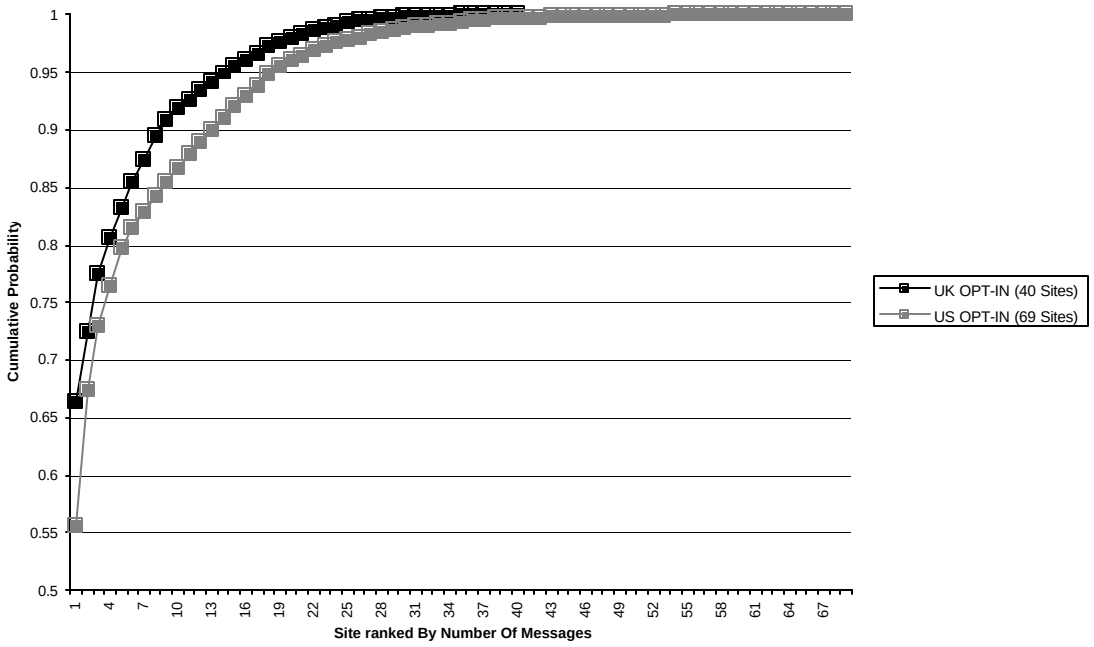
data for any secondary purpose. We applied the JMS field experiment methodology to 56 high traffic websites in the U.K. Out of the 56 websites, 40 U.K. websites allowed us to opt-in, and 25 websites allowed us to opt-out.

Figure 1: Mean Number of Email Messages Received



In a field experiment, Jamal, Maier and Sunder (JMS [2003]) constructed 200 identities (name, address, email address) and attempted to register twice on each of 100 high traffic websites in the U.S. In the opt-in registrations (n=69), JMS allowed the website to use personal data for both internal marketing purposes, and to sell personal data to external third parties. In the opt-out registrations (n=43), JMS did not allow the website to use personal data for any secondary purpose. JMS tracked the number of email messages received at each registered address over the twenty-six week period following the registration. We applied the JMS procedure on 56 U.K. websites regulated by EU privacy law. From our 56 websites in the U.K., 40 websites allowed an opt-in, and 25 websites allowed us to opt-out. Raw data for this chart are shown in Table 2. Figure 1 shows the average number of messages received by all U.S. and U.K. opt-in sites, average number of messages for all U.S. and U.K. opt-in sites except one outlier removed from both the U.S. and the U.K, and the average number of messages received from all U.S. and U.K. opt-out sites.

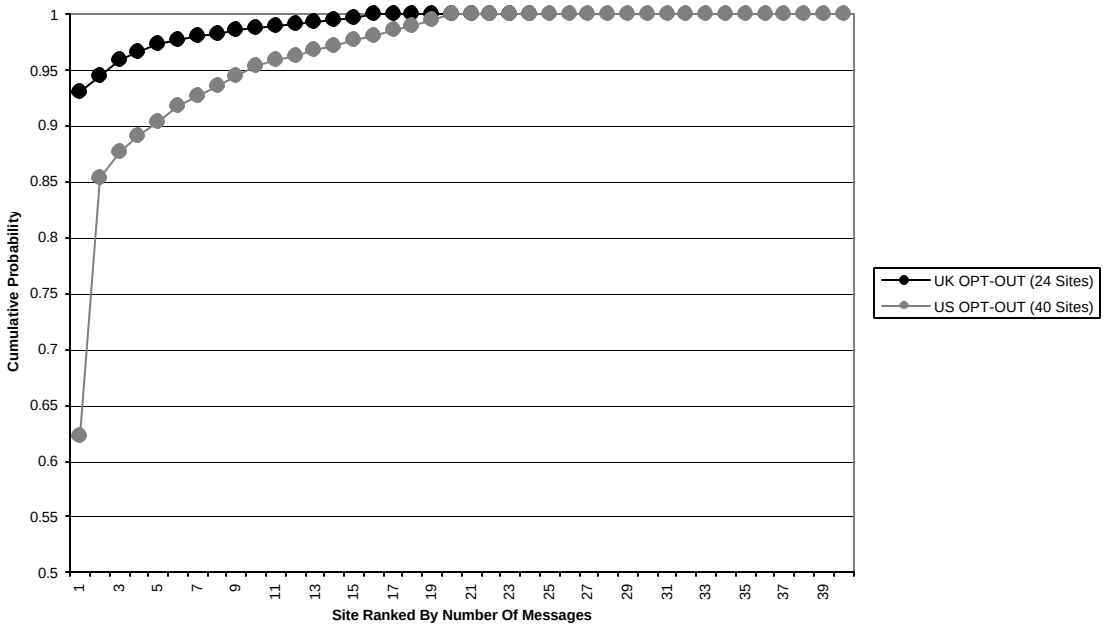
Figure 2: Cumulative Percent of Email Received From Volume Ranked Opt-In Websites in The U.S. (Self Regulation) and U.K. (Government Regulation)



In a field experiment, Jamal, Maier and Sunder (JMS [2003]) constructed 100 identities (name, address, email address) and attempted to register on each of 100 high traffic websites in the U.S. In the opt-in registrations JMS allowed the website to use their personal data for both internal marketing purposes, and to sell data to external third parties. Sixty-nine websites allowed JMS to register and opt-in. JMS tracked the number of email messages received in each registered address over a 26-week period. We replicate the JMS procedure in the U.K. for 56 high traffic websites. Forty of these websites allowed us to opt-in. We chart the number of email messages received at each of our opt-in and opt-out addresses.

In the U.S., one site alone, (an outlier), generated 56 percent of all opt-in messages indicated by the first circle on the chart. The five highest volume sites generated 80 percent of the total opt-in messages. In the U.K. (light square symbol in the figure), one site generated approximately 63 percent of all messages. The five highest volume sites generated 83 percent of the total opt-out messages. Note that the vertical scale has been truncated at 50 percent in order to highlight the differences in the 90-100 percent range.

Figure 3: Cumulative Percent of Email Received From Volume Ranked Opt-Out Websites in The U.S. (Self Regulation) and U.K. (Government Regulation)



In a field experiment, Jamal, Maier and Sunder (JMS [2003]) constructed 100 identities (name, address, email address) and attempted to register twice on each of 100 high traffic websites in the U.S. In the opt-out registrations JMS did not allow the website to use data for any secondary purpose. Out of the 100 websites, 43 allowed JMS to register and opt-out. JMS tracked the number of email messages received in each registered address over a 26-week period. We replicate the JMS procedure in the U.K. for 56 high traffic websites. Twenty-five U.K. websites allowed us to opt-out. We chart the number of email messages received at each of our opt-in and opt-out addresses. In the U.S., one site alone, (dark circle), generated 62 percent of all opt-out messages indicated by the first circle on the chart. The five highest volume sites generated 91 percent of the total opt-out messages. In the U.K. (light square symbol in the figure), one site generated approximately 93 percent of all messages. The five highest volume sites generated 97 percent of the total opt-out messages. Note that the vertical scale has been truncated at 50 percent in order to highlight the differences in the 90-100 percent range.

Appendix A

U.K. Data Protection Act 1984 (Amended in 1998 For Compliance With EU Privacy Law) – Can be obtained online at www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm

SCHEDULE 1: THE DATA PROTECTION PRINCIPLES

PART I: THE PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2 is met (requirements of informed consent), and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix B

Enforcement Activity By The U.K. Information Commissioner For the Five Year Period From 1997 - 2002

	1997/98	**1998/99**	**1999/00**	**2000/01**	**2001/02**
Total Budget	£ 3,661,690	£ 4,190,489	£ 4,721,666	£ 5,280,860	£ 8,244,982
# Of Staff	109	118	114	126	157
# Of Phone Inquiries	48,337	48,549	55,070	55,125	56,982
Total Complaints Received	4,178	3,653	5,166	8,875	12,479
Visits - Business Premises	471	700	388	480	448
Visits - Dwellings	313	319	199	235	411
Witness Statements Obtained	378	433	346	355	375
Interviews Under Caution	136	216	98	144	58
Court Prosecutions	38	59	145	23	66
Court Convictions (Guilty)	38	55	130	21	33

The Information Commissioner enforces and oversees the Data Protection Act 1998. The Commissioner is a U.K. independent supervisory authority reporting directly to the U.K. Parliament. The Commissioners mission is: "We shall develop respect for the private lives of individuals and encourage the openness and accountability of public authorities. Promoting good information handling practices and enforcing data protection and freedom of information legislation; and seeking to influence national and international thinking on privacy and information access issues."

This information on the Budget and Enforcement activity of the U.K. Information Commissioner was obtained from the Commissions annual reports which can be obtained at http://www.dataprotection.gov.uk/ar2001annrep/