DISSENTING STATEMENT OF COMMISSIONER ORSON SWINDLE
in *Privacy Online: Fair Information Practices in the Electronic Marketplace*
A Report to Congress

I dissent from this embarrassingly flawed Privacy Report and its conclusory yet sweeping legislative recommendation.

or unfounded fears of new technology? Is it the online dissemination of personal information or the offline availability of such information? How is the proposed solution related to the problem? Why is law enforcement against violations of posted privacy policies inadequate? Why not encourage consumers to vote with your mouse ? In light of the widespread adoption of privacy policies and developments in privacy protection technology, consumers can choose to make purchases at sites compatible with their privacy preferences and not use sites that are incompatible with their preferences. Consumers who feel very strongly about privacy can use technological tools to further enhance their privacy online, such as anonymizer programs or cookie crumblers, and may simply rely on information available online to make an offline purchase.

Isn t the real privacy problem the lack of information and education? This can be addressed by self-regulation. Legislation is not necessary.

I. WHAT DO THE SURVEY RESULTS SHOW?

sites post a privacy policy. (PR at 10). This also shows noteworthy progress from comparable 1999 figures of 44% and 81%. (.).

B. The Survey Provides a Unique Baseline for Measuring the Quality of Privacy Disclosures

manner also increases the number of sites that meet the 2000 Survey s full FIPPs standard to 27% (Random Sample) and 63% (Most Popular). *( )*.

II. PROBLEMS WITH THE REPORT S INTERPRETATION OF SURVEY RESULTS

A. The Report s Direct Comparisons to Earlier FIPPs Numbers Are Bogus

Regardless of the manner in which the qualitative measures of Notice, Choice, Access, and Security are combined or separated, the FIPPs figures from the 2000 Survey stand alone and are beyond the scope of earlier surveys. The Privacy Report s repeated comparison of full FIPPs numbers of 20% of the Random Sample and 42% of the Most Popular Group to what it calls similar figures of 10% and 22% from Professor Culnan s 1999 surveys is a misleading

indirectly encouraging Web sites not participating in seal programs to adopt privacy policies to better compete with sites that are. Instead, it leaps to the conclusion that the number of sites displaying seals means that enforcement is lacking and that government enforcement of new privacy regulations is the solution.

D. The Report Confirms the Exponential Growth in Online Commerce, but Misuses Consumer Confidence Surveys and Lost Sales Projections

The Privacy Report seeks to justify legislation and regulation on the ground that privacy concerns are limiting the commercial growth of the Internet. It does acknowledge the exponential growth that has occurred in recent years in the online economy. But it also boldly asserts that consumer fear about privacy likely translates into lost online sales due to lack of confidence in how personal data will be handled (PR at 2), and concludes that government intervention will reduce such lost sales. There is little empirical support for these conclusions.

1. Misuse of Consumer Confidence Surveys

Not surprisingly, the attention paid by the media and government to online privacy concerns is reflected in consumer surveys showing a general lack of confidence in online privacy protections. The Privacy Report, however, overstates the extent and significance of consumer concern about online privacy to support its call for government regulation. (PR at 2).

a. Odyssey Study Example

For example, the Privacy Report states that there is consumer unease about online privacy based on a recent study [by Odyssey] in which 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential, and 82% agreed that the government should regulate how online companies use personal information. (PR at 2). The Odyssey Study itself states that 47% of online households strongly agree, 35% somewhat agree, and 18% strongly disagree with the statement that government regulation is needed. The majority has arrived at its 82% figure by adding

---

Odyssey, (2000) (Odyssey Study) at 2.

positive response any consumer who has ever been dissuaded from making any purchase online from the relevant type of Web site. Positive responses therefore include consumers who may well have simply decided to make their online purchase from some other online retailer, thereby resulting in no lost online sale at all. Positive responses thus also include consumers who may well have been dissuaded from making a purchase in the relatively distant past but are now undeterred from making purchases online, which means that the responses could very well overstate the risk of current and future lost sales online due to privacy concerns. In fact, these results suggest that many consumers want information about privacy practices and that consumers can and do exercise choice based on their privacy preferences.

2. The Report s Reliance on Lost Sales Projections Is Misplaced

Nor are the lost sales projections relied upon by the majority valid justifications for government regulation of privacy. The Report s sweeping statements about consumer privacy fears likely resulting in billions of dollars of lost sales are based primarily on two consumer surveys conducted in mid-1999 or earlier. These surveys were the basis for estimates that sales lost to lack of consumer confidence in privacy protections were $2.8 billion in 1999 and could be as much as $18 billion by 2002.

i. Forrester Privacy Best Practice Report

The Privacy Report obtained the $2.8 billion estimate from a study that Forrester Research, Inc., released in September 1999. (PR at 2 n.16). The Forrester Report stated merely that concerned consumers who buy spend 21% less online than their more at-ease counterparts, leaving $2.8 billion on the table in 1999. It did not explain, however, how

---

The question in the IBM Privacy Survey asked: When you ve visited health, financial, insurance, or retail websites, have you EVER DECIDED NOT TO USE OR PURCHASE SOMETHING from this type of website because you weren t sure how they would use your personal information? IBM Multi-National Consumer Privacy Survey (Oct. 1999), prepared by Louis Harris & Associates, Inc. at 96, 99 (Exh. 5.1) (emphasis added) (capitalization in original).

Christopher M. Kelley, et al., , The Forrester Report (Sept. 1999) at 2.

Study.[4] That study provides the full scenario underlying the $18 billion lost sales projection. The projection rests on four assumptions: (1) the online [i]ndustry does nothing ; (2) [c]onsumers concerns [about Internet privacy] grow as media attention increases; (3) the Government implements legislation signaling to consumers that their concerns regarding privacy were justified; and (4) [c]onsumers fear impacts revenue.

Thus, the majority is relying on a projection of lost sales that is based on one assumption already proven wrong by the 2000 Survey that industry does nothing to protect privacy and another assumption that the government regulates privacy that has not yet come to pass. The Privacy Report s use of Jupiter s lost sales projection as the basis for recommending such legislation is indefensible.

In fact, the Jupiter Study appears to have used the projection to encourage self-regulation. That Study also concluded that consumers do not see government regulation as the solution to the online privacy issue. The vast majority of respondents to a Jupiter Consumer Survey 86 percent said that they would not trust a Web site with their privacy even if the government regulated it. The Jupiter study also found that only 14% of consumers asked to identify the top two factors that would positively affect their trust in Web sites with regard to their privacy indicated that they would more likely trust a Web site on privacy issues if the site were subject to government regulation. These figures clearly cut against the Privacy Report s recommendation for rulemaking.

---

[4] Michele Slack, Jupiter Communications, , , (June 1999).

Jupiter Study at 12-13 and Figure 9 (emphasis added).

Jupiter Study at 16.

. at 19.

. at 4.

suggests that many consumers do not act upon their fears or that they have generalized fears that are overcome by the provision of additional information by the sites with which they choose to do business. In fact, some of the studies cited by the majority s Privacy Report confirm that consumers fears about privacy are mingled with fears about the security of their credit card information. The Jupiter Study, for instance, reports that 78% of consumers surveyed stated that security of credit card information is the privacy issue that concerns them the most. Current encryption standards provide a lot of protection in this area, and it is probably less risky to use a credit card online than to use it in a restaurant or over the telephone. If consumers fears about security are exaggerated, then the solution is to find a way to reassure consumers by notice and education rather than promulgating rules that may restrict their choices.

III. WHAT DOES THE REPORT FAIL TO DO?

The Privacy Report fails to provide a reasoned basis for its legislative recommendation. As discussed above, it relies only on a one-sided interpretation of the 2000 Survey results and the existence of consumer concern about privacy. The Report fails to adequately address the alternatives to legislation. Its discussion of self-regulation does not give appropriate credit to self-regulatory efforts other than seal programs, nor does it address the continued development of privacy-related technology.

Most fundamentally, the Privacy Report fails to pose and to answer basic questions that all regulators and lawmakers should consider before embarking on extensive regulation that could severely stifle the New Economy. Shockingly, there is absolutely no consideration of the costs and benefits of regulation; nor the effects on competition and consumer choice; nor the experience to date with government regulation of privacy; nor constitutional implications and concerns; nor how this vague and vast mandate will be enforced.

Respondents were asked to choose the top three factors that most concerned them. Jupiter Study at 3-4.

news release seen by more than four million Americans on protecting privacy while shopping online for Christmas.

The American Electronics Association (AEA) sponsored a series of seminars in January 2000, entitled E-Commerce Privacy: Building Customer Trust. AEA has established a significant business relationship with BBBOnline in which a significant discount is offered to its 3,400 member companies who gain certification under BBBOnline s strenuous online privacy program.

The Direct Marketing Association (DMA) Privacy Promise was successfully launched on July 1, 1999. Under DMA s Privacy Promise program, its members commit to provide customers with notice of their right to opt out of information exchanges, honor opt-out requests, maintain an in-house file of consumers who have asked not to be recontacted, and use DMA s mail and telephone do-not-call lists when prospecting. DMA membership is contingent on compliance with the Privacy Promise. Fewer than 1% of DMA members refused to comply. More than 2,000 DMA member companies signed up, making this the largest self-regulatory program based on numbers of participants. DMA has revised its Privacy Policy Generator to reflect the most current issues, making it easier for companies to explain to consumers their access policies, their enforcement programs, and their relationship with ad servers.

In April 2000, the Association for Competitive Technology (ACT) unveiled Net Privacy: You ve Got the Power, a multi-faceted campaign designed to educate consumers on how to protect their privacy online. The campaign was launched with public service advertisements educating readers about online privacy and directing them to www.NetPrivacyPower.org. In addition to the Web site, the campaign includes print advertising, online advertising, direct mail and email.

The U.S. Chamber of Commerce continues to reach out through a variety of

preferences in sharing personally identifiable information with Web sites, there are many other privacy products.

Those tools can be divided into two types: those that protect or shield a browsing consumer s identity, and those that help the consumer negotiate what information her or she wishes to share. Anonymizer technology like anonymizer.com and Zero Knowledge Systems give a consumer anonymity on the Web. Infomediaries allow a consumer to exercise choice in the types of personally identifiable information that is shared each time a Web site is visited. A consumer can create a personal profile that enables the technology to negotiate the release of information specified by the consumer.

For example, AllAdvantage.com acts as an agent on behalf of consumers to create a market for the use of their information without consumers losing control over their information. Digital Me from Novell stores a consumer s personal information and uses it to automatically fill out forms at Web sites, allowing the consumer to review what is being submitted. Persona by Priva Seek allows a consumer to surf anonymously and sell his or her specified, personally identifiable information in exchange for discounts.

1. Notice

Notice seems less likely to impose tremendous costs and may have many benefits. The 2000 Survey results show that Notice already is widely provided, but there appear to be problems with the clarity and understandability of privacy disclosures. (PR at 24-28). To the extent that Notice is clearly provided, firms can compete on the basis of their privacy policies, and the privacy preferences of one group of consumers need not limit the choices of other groups. Industry adherence to a set of best practice guidelines for Notice should be attempted and assessed before we resort to legislation. To the extent that online companies do not provide clear notice, consumers who care about privacy should shop elsewhere. The workings of the market are preferable to the workings of government.

2. Choice

As described in the 2000 Survey and the Privacy Report s legislative recommendation, Choice is not the free-market version of choice that relies on informing the consumer so that the consumer can choose not to use a site if he or she dislikes the privacy policy. Rather than promoting informed comparison shopping for acceptable privacy practices, the Commission asks Congress to impose a mandated version of Choice that appears to entitle the consumer to continue to use any site, but gives the consumer control over the site s internal and external uses of his or her personal information. (PR at 36).

Like other aspects of the Commission s recommendation, Mandated Choice raises policy issues that the Report simply ignores. What are the likely effects on online commerce of Mandated Choice? Would sites have to extend the same level of services and benefits to all consumers, regardless of whether some are unwilling to provide information? To the extent sites rely on the sale or use of information to offset the costs of providing services, would they discontinue services to all or to some consumers? Would all consumers have to pay more for services previously offset by the sale or use of information? Could sites shift costs only to those consumers who demand a higher level of privacy, whether in the form of fees for using the site or by reducing the level of benefits and services offered to those who choose a higher level of

privacy? Or is privacy an absolute right so that all participants in online commerce retailers and consumers should bear the costs of Mandated Choice exercised by some consumers? If so, in the name of Choice, this legislation may reduce the choices available to consumers in the online market.

These are fundamental policy decisions, not mere issues of implementation that can be resolved later when unelected bureaucrats decide how to regulate the online world. Legislation adopting Mandated Choice will have consequences for online commerce that should be understood before Mandated Choice is written into law.

3. Access

The majority recommends that Congress enact legislation requiring all commercial, consumer-oriented Web sites to provide reasonable access to consumers personal information. Again, the majority does not ask why the 2000 Survey s Access numbers are not as high as the majority evidently expected them to be. As the Advisory Committee found, sites may actually provide Access yet not specifically address it in a notice. (Advisory Committee Report at 4). For example, access may be provided by e-mail to information about what the customer ordered, its price, and where it is to be delivered. The 2000 Survey did not count this type of access unless it was described in a privacy disclosure. Nor did the 2000 Survey take account of the type or sensitivity of information collected by sites that fail to provide Access. To the extent that the majority may be prepared to treat reasonable Access as no Access under some circumstances, it is noteworthy that the 2000 Survey gave no credit for no Access.

The Advisory Committee s report discusses the costs and risks of Access, particularly the problem that the access principle sometimes pits privacy against privacy. . . . Privacy is lost if a security failure results in access being granted to the wrong person. (Advisory Committee

Interestingly, the Advisory Committee heard estimates from Web companies that less than one percent of customers who are offered access actually take advantage of the offer. Concurring Statement of Stewart Baker, Steptoe & Johnson LLP, appended to Advisory Committee Report.

Advisory Committee members that the government should mandate security standards or that the Commission should be setting security standards.

5. Competitive Effects

This Report is from the leading antitrust agency, yet it contains no consideration of the competitive effects of the remarkably broad legislation it proposes. The Report ignores the likely result that government-created standards for all consumer-oriented, commercial Web sites may cause some online companies, particularly smaller ones, to limit their online services or exit the online marketplace altogether. What are the likely effects of the majority s proposed legislation on consumers and competition? Will the advantages of the bigger players be enhanced, while small entrepreneurs face artificial and costly barriers to entry? How will that affect the innovation and provision of services that consumers want? What costs will it impose on consumers who do not care about privacy or are willing to make some tradeoffs?

6. Constitutional Issues

The Privacy Report does not address the fundamental question whether a statute that incorporates its recommendations would violate the First Amendment to the United States Constitution. The majority recommends that the Congress impose broad restrictions on the sale to a third party of personal information collected online by any consumer-oriented commercial Web site. (PR at 38). Both the courts and the Commission have recognized that sales of personal information to third parties are accorded the same level of Constitutional protection as commercial speech. *&* , . . , ., 472 U.S. 749, 758-59 (1985) (plurality opinion); ., FTC Dkt. No. 9255, slip op. at 33-37 (Feb. 10, 2000). To determine whether a government restriction on commercial speech passes constitutional muster, a court must examine: (1) whether the expression at issue concerns lawful activity and is not misleading; (2) whether the asserted governmental interest supporting the restriction is substantial; (3) whether the regulation directly and materially advances the

Concurring Statement of Stewart Baker, Steptoe & Johnson LLP, appended to Advisory Committee Report.

harbor program that relies on the creativity of industry to come up with self-regulatory guidelines that satisfy the requirements imposed by statute.

8. Offline Privacy

As Commissioner Leary thoughtfully explains in his concurring and dissenting statement appended to the Privacy Report, online regulation of privacy has implications for the offline world. The Privacy Report acknowledges, but does not analyze, the issue in an ominously vague footnote promising that significant attention to offline privacy issues is warranted. (PR at 3 n.23).

IV. WHERE DO WE GO FROM HERE?

The Privacy Report stands as the majority s justification for the recommendation to legislate privacy a dramatic reversal in position for the Commission and a mandate for the commercial online world to comply with the government s interpretation of all four fair information practice principles. Yet the Report is extremely flawed in its presentation of fact, its analytical logic, and its conclusions. This is no way to create good law.

Everyone recognizes that there are imperfections and deficiencies in the state of privacy on the Internet, but let us not make the search for the perfect the enemy of the good. The private sector is continuing to address consumer concerns about privacy, because it is in industry s interest to do so. Congress may wish to enact more limited legislation or may continue to rely on enforcement agencies and corporate leadership. Now is not the time for legislation, but if legislation cannot be avoided, then a basic standard for a readily understandable, clear and conspicuous Notice combined with a campaign by industry and government to continue to educate consumers about the tools at their disposal would go a long way to protect consumer privacy by ensuring that consumers could compare privacy policies and make informed choices based on their privacy preferences. If there is to be legislation, it should go no further than Notice. In light of the 2000 Survey s positive findings about the broad-based implementation of Notice by Web sites, mandating Notice seems less likely to be fraught with severe, unintended consequences for online commerce. Notice allows consumers to exercise informed choice to