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.[1] In an unwarranted reversal of its earlier acceptance of a self-regulatory approach, a majority of the Commission recommends that Congress require **all** consumer-oriented commercial Web sites that collect personal identifying information from consumers to adopt government-prescribed versions of all four fair information practice principles ("FIPPs"): Notice, Choice, Access, and Security.[2] The majority abandons a self-regulatory approach in favor of extensive government regulation, despite continued progress in self-regulation.

The majority recommends that Congress give rulemaking authority to an "implementing agency" (presumably the Commission) to define the proposed legislative requirements "with greater specificity," to "expand on what constitutes 'reasonable access' and 'adequate security'" and to "examine the specific contours of the Choice requirement . . ." (Privacy Report ["PR"] at 37). In some cases, the Report explains, the agency engaged in rulemaking might determine that "reasonable access" means "no access" despite the recommended statutory direction to provide access. (*Id.*). The Commission owes it to Congress — and the public — to comment more specifically on what it has in mind before it recommends legislation that requires all consumer-oriented commercial Web sites to comply with breathtakingly broad laws whose details will be filled in later during the rulemaking process.

Most disturbing, the Privacy Report is devoid of any consideration of the costs of legislation in comparison to the asserted benefits of enhancing consumer confidence and

[1]To assist readers, a list of the topics I address is appended to my dissenting statement.

[2]While this is a reversal for the Commission, Commissioner Anthony has consistently preferred a legislative approach. *See* Statement of Commissioner Sheila F. Anthony, Concurring in Part and Dissenting in Part, *Self-Regulation and Privacy Online* (July 1999), available at <http://www.ftc.gov/os/1999/9907/index.htm#13>.

allowing electronic commerce to reach its full potential. Instead, it relies on skewed descriptions of the results of the Commission's 2000 Survey and studies showing consumer concern about privacy as the basis for a remarkably broad legislative recommendation. It does not consider whether legislation will address consumer confidence problems and why legislation is preferable to alternative approaches that rely on market forces, industry efforts, and enforcement of existing laws.

In fact, the 2000 Survey demonstrates continued noteworthy growth in the display of privacy notices and, for the first time, provides a qualitative assessment of the content of privacy notices. The survey results, despite their flaws, show continued development of self-regulatory privacy policies that are, for the most part, not yet comprehensive when measured against the 2000 Survey yardstick. **Why?** As discussed below, the Privacy Report makes no attempt to answer this vital question, but instead leaps to the conclusion that legislation is needed.

The majority's Report concludes that the 2000 Survey numbers "demonstrate" that industry self-regulatory efforts are insufficient. (PR at 35). It makes no attempt to determine **why** the figures warrant changing course to advocate legislation. Instead, the Report concludes that legislation is needed because self-regulation "**cannot ensure that the online marketplace as a whole will emulate the standards adopted by industry leaders.**" (PR Executive Summary at ii-iii) (emphasis added). When has self-regulation ever ensured that every member of an industry will adopt industry standards? If this is the Commission's new standard for successful self-regulation, then no numbers can ever be high enough to meet it. Using such logic leads inevitably to government regulation.

To the extent that Access and Security disclosures are less prevalent than expected, the Survey results are consistent with the implementation difficulties identified by the Advisory

Committee on Access and Security in that Committee's report.[3] The Choice figures, while much higher than the Access and Security figures, also are not surprising in light of the unanticipated complexities of implementing a far more limited version of opt-out Choice required by the Gramm-Leach-Bliley ("G-L-B") Act for protecting the privacy of consumers' financial information.[4] Reports that many companies are exiting the business of providing services to children online to avoid the burdens of complying with regulations issued under the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501 *et seq.*, also should raise a red flag about the wisdom of proceeding to mandate Choice and Access for all commercial consumer-oriented Web sites.[5]

Nor did the 2000 Survey attempt to measure whether sites actually provide Access and Security; rather, it gauged only whether disclosures addressed these issues. And the 2000

[3]In 1999, the Commission established an Advisory Committee on Online Access and Security to provide advice and recommendations to the Commission regarding implementation of reasonable access and adequate security by domestic commercial Web sites. The Committee provided the final version of its report to the Commission on May 15, 2000, describing options for implementing reasonable access to, and adequate security for, personal information collected online and the costs and benefits of each option. The Advisory Committee report is appended to the Privacy Report.

[4]The Commission, along with other agencies involved in implementing the G-L-B Act's privacy provisions, has found it necessary to extend the deadline for compliance with the implementing regulations by more than seven additional months to provide sufficient time for financial institutions to establish new policies, procedures, and systems for implementing regulatory requirements. Federal Trade Commission, Final Rule, Privacy of Consumer Financial Information, available at <http://www.ftc.gov/os/2000/05/glb000512.pdf>.

[5]The COPPA regulations require detailed Notice; Access, including the ability to review, correct, and delete information maintained by the site; and a form of opt-in mandated Choice (verifiable parental consent). 16 C.F.R. §§ 312.4, 312.6(a)(1), 312.6(a)(2), 312.5(a), 312.5(b). The regulations went into effect on April 21, 2000, and already press reports state that some small online companies have stopped providing services to children because implementation of COPPA's requirements is too costly. *See, e.g.*, "New Children's Privacy Rules Pose Obstacles for Some Sites," *The Wall Street Journal* (April 24, 2000) at B-8 (reporting one attorney's estimate that it will cost her clients between $60,000 and $100,000 annually to meet COPPA standards); "New privacy act spurs Web sites to oust children," William Glanz, *The Washington Times* (April 20, 2000), available at < *See also* "COPPA Lets Steam out of Thomas," Declan McCullagh, *Wired News* (May 16, 2000), available at <wysiwyg://1/http://www.wired.com/news/politics/0,1283,36325,00.html>.

Survey certainly did not give any credit for "No Access," even though the majority indicates it might consider no access to be "reasonable Access" in some instances.

Why does the Privacy Report not analyze why the 2000 Survey figures are too low to avert legislation? Perhaps it is because the 2000 Survey results, like the Advisory Committee's report, are not really the basis for the Commission's startling legislative recommendation. The Commission has barely had time to review, much less digest, the detailed report issued by the Advisory Committee earlier this week, including the very illuminating statements of individual members of the Committee.[6] Apparently, the majority views the Committee's report as something for an implementing agency to consider **later**, when it writes regulations detailing how **all commercial, consumer-oriented Web sites** are to comply with laws requiring them to provide "reasonable access" and "reasonable security." I, on the other hand, think the Advisory Committee's report is an incredibly valuable contribution to self-regulation and urge Congress to consider it fully before enacting legislation — something the Commission has failed to do before recommending legislation. Notably, the Advisory Committee's report does **not** recommend government action.

Nor do there appear to be independent reasons supporting the majority's broad legislative recommendation. Legislation should be reserved for problems that the market cannot fix on its own and should not be adopted without consideration of the problems legislation may create by, for example, imposing costs or other unintended consequences that could severely stifle the thriving New Economy. What is the problem to be solved here? Is it abuse of privacy online

[6]Stewart Baker points out in his concurring statement that the FTC refused to share the results of the 2000 Survey with the members of the Advisory Committee because the survey results were too confidential. Nonetheless, details about the survey results and the staff recommendation for legislation leaked to The Wall Street Journal, as reported on Thursday, May 11, 2000, and confirmed by FTC spokesman Eric London, indicated that the Commission's study of online privacy ignored the lessons of the Advisory Committee's report. Concurring Statement of Stewart Baker, Steptoe & Johnson LLP, Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security (May 15, 2000). *See also* Separate Statement of Jerry Cerasale appended to Advisory Committee Report (noting that any recommendation for government access likely was determined before the Committee issued its report).

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?

A. The Survey Shows Continued, Significant Progress in the Frequency of Privacy Disclosures

It is critical to recognize what the majority's Report does and does not do. First, it presents a survey that is a one-time snapshot of the characteristics of privacy disclosures provided online in late February 2000. The survey results show noteworthy progress on two measurements that are directly comparable to similar figures from surveys described to Congress in the Commission's 1998 and 1999 reports on online privacy: the posting of privacy disclosures (or information statements) and the posting of privacy policies. **The first set of these comparative figures, displayed in Figure 1 of the Privacy Report, shows that 88% of Web sites in the Random Sample post at least one privacy disclosure and that 100% of the Most Popular Web sites post at least one privacy disclosure.** (PR at 10, Appendix C, Table 2a). These figures rose to 66% and 93% respectively last year, up from 14% and 71% respectively in 1998. (PR at 11, Figure 1). **The second set of comparative figures shows that fully 62% of Web sites in the Random Sample and 97% of the Most Popular Web**

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

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

Next, the 2000 Survey presents a unique and demanding measurement of the quality and detail of privacy disclosures based on the four FIPPs. When the 2000 Survey gives credit for "Notice," it requires a level of notice that satisfies four distinct requirements: (1) the site posts a privacy policy; (2) it says anything about what specific personal information it collects; (3) it says anything about how the site may use personal information internally; and (4) it says anything about whether it discloses personal information to third parties. When the 2000 Survey results refer to "Choice," it means that the site did two things: (1) it stated that it provided the consumer an option to authorize or agree to the site's use of personal information to send communications back to the consumer (or stated that it did not use personal information in this way); and (2) it stated that it provided an option to authorize or agree to the disclosure of personal identifying information to third parties (or stated that it did not disclose personal identifying information to third parties).

In partial recognition of the complexities of these issues, Access and Security were measured by simpler standards. When the 2000 Survey concludes that a site provided "Access," it means that the site stated that it did at least one of three things: it allowed consumers to review, delete, or correct at least some personal information. "Security" means that the site explicitly stated that it takes steps to provide security. As the Privacy Report acknowledges, providing security is more important than disclosing it.[7] **The 2000 Survey did not attempt to measure whether sites actually provide security (or access, for that matter), but only whether privacy disclosures addressed them in the parameters described above.**

[7]PR at 19; *see also* Advisory Committee Report at 19-20.

C. Disclosures Addressing Individual Fair Information Practice Principles Are Widespread

NOTICE: The survey results show that **55%** of sites in the Random Sample and **89%** of the Most Popular sites meet all four Notice requirements. (PR Appendix C, Table 4).

CHOICE: **82%** of the sites in the Random Sample and **98%** of the Most Popular sites provide some form of choice for either sending communications to customers or disclosing information to third parties. (PR Appendix C, Table 10). **50%** of the Random Sample sites provide both types of choice, as do **67%** of the sites in the Most Popular Group. (PR Appendix C, Table 4).

ACCESS: **43%** of the Random Sample sites and **83%** of the Most Popular Group sites provide disclosures indicating that they provide some form of access. (PR Appendix C, Table 4).

SECURITY: **55%** of the Random Sample sites and **74%** of the Most Popular Group sites display a statement that the site takes steps to provide security. (PR Appendix C, Table 4).

Thus, when looked at in terms of adherence to individual fair information practice principles, the Random Sample numbers are fairly high and the Most Popular Group figures are substantially higher.

D. Comprehensive Privacy Policies that Provide All Four Elements of FIPPs Are Less Common

When the Privacy Report combines all four of the 2000 Survey's Notice, Choice, Access, and Security measurements to determine what sites have disclosures satisfying all four fair information practice principles, however, the results are much lower: **20%** of the Random Sample Web sites and **42%** of the Most Popular Web sites. (PR Appendix C, Table 4). If the Access and Security measurements are not considered, then **41%** of the sites in the Random Sample and **60%** of the Most Popular sites provide the four-element Notice and both types of Choice. (*Id)*. These numbers rise even more when sites are credited for providing choice either for internal uses or for disclosures to third parties: **54 %** of sites in the Random Sample and **87%** in the Most Popular Group. (PR Appendix C, Table 10). Treating Choice in this

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

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 apples-to-oranges comparison, because the 1999 surveys did not define Notice, Choice, Access, and Security to include the more demanding elements required by the Privacy 2000 survey. (PR at 12 nn. 76-77).

As acknowledged in footnotes 79 and 80 of the Privacy Report, the scoring models are not identical because the surveys asked different questions. **Using the most comparable approach possible in light of this significant limitation, the 2000 Survey's full FIPPs numbers rise to 25% and 57%. This apples-to-apples comparison shows a dramatic one-year improvement.** Nonetheless, the majority's Report chooses not to highlight this more direct comparison, instead measuring the 20% of the Random Sample Web sites that implement **all of the 2000 Survey's specified elements** for Notice, Choice, Access and Security against the 1999 survey that found 10% of sites had posted disclosures addressing **at least one element** of Notice, Choice, Access, and Security. *(See* PR Executive Summary at i).

B. Measuring Success on the Basis of Full FIPPs Is Irrational

Based on the many difficulties of implementing Access and Security, discussed in detail below, the Privacy Report's use of full FIPPs as the yardstick for success is irrational. It should be noted that even in the sensitive area of protecting personal financial information, the Congress did not insist on all four FIPPs in the G-L-B Act. Once beyond sensitive financial and medical information, the importance of Access arguably diminishes. Had the 2000 Survey

actually given credit for the majority's concession that in some cases "reasonable Access" might mean "no Access," the Access and full FIPPs numbers would be dramatically improved. Moreover, as discussed below in section III.C.4, Access and Security disclosures do not reflect whether a Web site actually provides Access and Security.

C. Equating Self-Regulatory Enforcement with the Prevalence of Seal Programs Is Misleading

Another striking feature of the Privacy Report is that, without analysis, it equates seal programs with enforcement and concludes that self-regulation has failed because the results of this first-time survey of the prevalence of participation in seal programs show that **8%** of Web sites in the Random Sample and **45%** in the Most Popular Group display privacy seals. The weighted analysis figure, which reflects how often consumers surfing the Random Sample Web sites are likely to encounter a privacy seal, is **36%.** (PR Appendix C, Table 14a). **Despite the fact that nearly one-half of the most frequently visited sites use a seal program, the Report states flatly that "the enforcement mechanism so crucial to the success and credibility of self-regulation is *absent*."** (PR at 35) (emphasis added).

Moreover, the FTC already has power to take action against violations of privacy policies. The Privacy Report does not comment on the FTC's challenges to privacy policies that violate Section 5 of the FTC Act and how often such government enforcement actually has been needed.

Once again, the Privacy Report fails to ask "why?" Instead of considering **why** participation in seal programs is more than five times higher among the Most Popular Web sites than among the Random Sample sites, the majority simply concludes that the presence of seal programs on the Web is "not significant." (PR at 6). Nowhere does the Report discuss the costs of participating in a seal program, such as fees charged by the program, the time involved in applying and being granted approval to use a seal, and the costs of implementing seal program requirements. Nor does the Report ask whether the prevalence of seal programs may reflect how frequently consumers seek out and rely on privacy seals before purchasing from an online retailer, or whether seal programs may have positive effects on online privacy by

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.[8] The majority has arrived at its 82% figure by adding

[8]Odyssey, *Consumers' Internet Privacy Concerns: Lip Service or Limiting Factor?* (2000) ("Odyssey Study") at 2.

the percentages of online households that strongly agreed and somewhat agreed, something that the Odyssey authors themselves did not do.

Moreover, the Odyssey survey's method of describing consumers' views is unusual and somewhat biased in favor of "agree" responses, because it gives two possible answers that use the word "agree" and only one possible answer to "disagree." (Odyssey Study at 2, Chart 1). Typically in a survey the points used in a three-point scale would be labeled something like: (1) agree; (2) neither agree nor disagree; and (3) disagree. A typical four-point scale would have labels along the lines of: (1) strongly agree; (2) somewhat agree; (3) somewhat disagree; and (4) strongly disagree. In the Odyssey survey, only one category — "strongly disagree" — is available for consumers who have only weak opinions but tend to disagree. Since they do not "strongly" disagree, such consumers might say they "somewhat agree," even though that is not an accurate portrayal of their views. The Odyssey survey method pushes consumers to "agree" categories and captures consumers in the "somewhat agree" category who may simply tend more to "somewhat disagree" (a choice not offered by the survey). In these circumstances, the Privacy Report's addition of the "strongly agree" and "somewhat agree" responses is very misleading.

b. IBM Privacy Survey Example

Regardless of the extent to which consumers are concerned about privacy online, the available data do not support the conclusion that these concerns are causing any significant lost online sales. The Report also cites the IBM Privacy Survey as support for the proposition that "surveys show that those consumers most concerned about threats to their privacy online are the least likely to engage in online commerce." (PR at 2 n.14). Specifically, the Report observes that "57% of Internet users have decided not to use or purchase something from a retail Web site because they were not sure how the site would use their personal information." (PR at 15 n.84).

On its face, the IBM Privacy Survey does not demonstrate that there have been or will be a significant number of lost sales online because of privacy concerns. The survey treats as a

positive response any consumer who has **ever** been dissuaded from making **any** purchase online from the relevant type of Web site.[9] 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 *do* buy spend 21% less online than their more at-ease counterparts, leaving $2.8 billion on the table in 1999."[10] It did not explain, however, how

[9]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).

[10]Christopher M. Kelley, et al., *The Privacy Best Practice*, The Forrester Report (Sept. 1999) at 2.

this estimate was calculated, much less reveal the underlying data on which its estimate was based. In fact, the 21% figure was based on what this group of consumers reported spending during the three-month period prior to the survey.[11] Forrester has not updated these data for 2000. **The Forrester lost sales projection therefore does not reflect changes that have occurred in online commerce since mid-1999.**

ii. Jupiter Proactive Online Privacy Study

Even worse, the Report relies — as a basis for legislation — on a projection of "potential losses of up to $18 billion by 2002 (as compared to a projected total of $40 billion in online sales), if nothing is done to allay consumer concerns." (PR at 2). The Report cites to an overview of a study that Jupiter Research Services released in June 1999. (PR at 2 n.17).[12] **The data supporting the statements in the Jupiter Study are at least a year old and, since industry self-regulation has made significant progress since June 1999, the Jupiter lost sales projections are clearly not applicable today**.[13]

The overview on which the Privacy Report relies does state that Jupiter projects a "[l]oss of $18 billion in Commerce Revenue" due to privacy concerns. But the overview also explains that the forecast is that such revenue losses will be suffered "**unless** [Web sites] take a more proactive approach and engage in an informed dialogue to shape and allay consumers' fears" (emphasis added) and contains a heading that states "A Do-Nothing Approach Will Lead to Significant Revenue Loss."

Here, the Report makes a quantum leap in logic, misleading Congress by going beyond simply selectively citing the Jupiter Study overview. It fails to consider the complete Jupiter

[11]Conversation between my staff and Christopher M. Kelley, Forrester Research (May 17, 2000).

[12]Specifically, the Report cites a press item dated August 17, 1999, which, in turn, quotes from the Jupiter Study. The Report also cites the overview of the Jupiter Study available at Jupiter's Web site to registered users. (PR at 2 n.17).

[13]The online overview of the Jupiter Study warns purchasers of its research that "[a]ll opinions and projections are based on Jupiter's judgment at the time of the publication and are subject to change."

Study.[14] 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."[15]**

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.[16] 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."[17] **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."[18]** These figures clearly cut against the Privacy Report's recommendation for rulemaking.

---

[14]Michele Slack, Jupiter Communications, *Proactive Online Privacy, Scripting an Informed Dialogue to Allay Consumers' Fears* (June 1999).

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

[16]*See* Jupiter Study at 16.

[17]*Id.* at 19.

[18]*Id.* at 4.

iii. Legislation Is Not Needed and in Fact May Cause Lost Sales

Assuming for the sake of argument that privacy concerns are causing some lost online sales, it is far from clear that government intervention is the appropriate response. First, some of the same consumer surveys that purport to show that privacy concerns are causing lost online sales also appear to indicate that government intervention is not needed to allay consumers' privacy concerns.[19] Moreover, government regulation of online privacy obviously will impose substantial costs on online sellers that might very well reduce their online sales or induce firms to offer fewer products for sale or go out of business entirely — an offsetting reduction in online commerce that the Report entirely ignores.

iv. "Lost" Sales Are Not Really Lost

Finally, a lost online sale is not a complete loss to the economy. Again, assuming for the sake of argument that consumers have been dissuaded from making purchases online because of privacy concerns, the most likely response of these consumers would be to purchase the same item from an offline retailer. Of course, switching to an offline retailer in this situation may not be the optimal economic outcome, because transaction costs might be lower if consumers make the purchase online. Offline retailers might be able to free-ride on the services provided by online retailers. Nevertheless, the fundamental point remains that overlooking offline sales that offset a lost online sale overstates the economic effect of the lost online sale.

v. The Meaning of Surveys Showing Consumer Unease Is Unclear

Consumer surveys often are poor predictors of consumers' actual behavior. The growth of online commerce despite growing consumer awareness and concern about online privacy

[19]For example, the Odyssey study reports that "82% of online shoppers say they would be more likely to shop at an online retailer that promised not to reveal their personal information to third parties." Odyssey Study at 3. The study notes that for such privacy promises to be credible, it is "absolutely essential" that online retailers communicate clearly to consumers what privacy policies are in place and adhere to those policies. *Id.* at 3-4. The study concludes that "it appears that the security and privacy policies of successful online retailers today are adequate to provide for continued growth in electronic commerce." *Id.* at 4. Consequently, the Odyssey study does not support the majority's position that more government regulation is needed to prevent lost sales resulting from online privacy concerns.

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.[20] 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.

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

A. The Report Does Not Adequately Credit Self-Regulatory Efforts

The Privacy Report's emphasis on seal programs overshadows other corporate efforts. **Corporate leaders** including IBM, Microsoft, Disney, Intel, Procter and Gamble, Novell, and Compaq have voluntarily committed to requiring their advertising partners to post high-quality privacy policies in order to receive advertising monies.

Microsoft has committed to developing business and consumer tools based on the Platform for Privacy Practices Protocol ("P3P"). The business tool known as the Privacy Statement Wizard is intended to enhance the ability of Web site operators to present their privacy statements both as human and as machine-readable documents. A related consumer tool, the Privacy Manager Wizard, is intended to enhance consumers' abilities to state their personal information privacy preferences. An early version of the Privacy Statement Wizard has been on the market for just over a year and has allowed over 15,000 companies to craft their own online privacy practices by answering a questionnaire.

Associations also have stepped up to the plate. On May 8, 2000, the CEOs of theglobe.com, Yahoo!, Inc., America Online, Lycos, Inktomi , Excite@Home**,** eBay, DoubleClick, Amazon.com, and EMusic.com, wrote a letter on behalf of NetCoalition.com to the CEOs of the Top 500 Web sites urging them to take the initiative to ensure that their companies establish and promote the adoption and implementation of rigorous voluntary privacy policies. NetCoalition.com led the way during the 1999 holiday shopping season, sponsoring a "Consumer Privacy Education Campaign" to empower Internet users with practical information about online privacy. The campaign included over 50 million impressions with banner ads and site impressions.

The Online Privacy Alliance ("OPA") continues to play a leading role serving as an industry coordinator and a general information resource. The OPA has taken significant strides toward alerting consumers and businesses about the value of privacy protection, as well as how to provide substantive protective measures. In December 1999, OPA disseminated a video

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 communication methods to state and local chambers to educate them about the importance of

robust online privacy practices. The Chamber has worked closely with OPA and NetCoalition to educate trade associations not in the information-technology area regarding the need for their active involvement in educating their own members about the importance of online privacy.

In October and November 1999, the Software & Information Industry Association ("SIIA") undertook a comprehensive outreach program in which it contacted all of its member companies that did not have a privacy policy linked from the company home page. SIIA sent each company a letter encouraging them to develop fair information practices and to post a privacy policy online. In addition, SIIA provided each company with resources and information through an online "toolkit" on its web site and devoted the entire April issue of its association magazine to the issue of online privacy.

The Electronic Retailing Association ("ERA") joined 35 associations in March, 2000 to urge each of their member companies to post a simple, straightforward privacy policy. As a condition of membership, ERA member companies are required to abide by ERA's Online Marketing Guidelines.

Many other associations that have endorsed and promoted self-regulatory solutions to online privacy including the Information Technology Association of America ("ITAA"), Information Technology Industry Council ("ITI"), Business Software Alliance ("BSA"), Computer & Communications Industry Association ("CCIA"), Computer Systems Policy Project ("CSPP"), Consumer Electronics Association ("CEA"), Electronic Industries Alliance ("EIA"), Semiconductor Industry Association ("SIA"), and the Telecommunications Industry Association ("TIA").

My discussion of these organizations is by no means intended to be comprehensive, but merely to demonstrate the extent to which the majority's Privacy Report ignores ongoing, significant industry self-regulation and promotion of privacy online.

B. The Report Ignores Developments in Technology

The market for privacy protection is growing and companies are responding with a host of technological tools. In addition to P3P, which will allow consumers to communicate their

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.

Technology can be one part of the solution to consumers' online privacy concerns. But the majority's Privacy Report does not consider the existence, or the likely impact of, such technological tools on consumer privacy online before recommending a legislative attempt to address consumer concerns. The market is working here: consumers are demanding tools to protect privacy and merchants are competing to provide them.

C. The Report Fails to Identify and Consider the Costs and Benefits of Proposed Legislation

The most fundamental flaw in the Privacy Report is its failure to address the costs and benefits of the legislation it proposes. While I cannot undertake a comprehensive analysis myself, a few observations are appropriate.

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."**[21]

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

[21]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.

Report at 15). Indeed, "[g]iving access to the wrong person could turn a privacy policy into an anti-privacy policy." (*Id.* at 4). In light of this, liability concerns may be preventing sites from providing Access. The Advisory Committee's report also observes that authentication of a consumer's identity before allowing that consumer Access could have considerable costs, including to the consumer's ability to remain anonymous. *(Id.)* Given the complexities and risks of Access, it is not surprising that Web sites have not implemented Access more broadly. Unlike the Commission, some may have been waiting to consider the findings of the Advisory Committee.

4. Security

As the Advisory Committee observes (and the Commission acknowledges in footnote 192 of the Privacy Report), **it is impossible to judge the adequacy of Web site security by surveying the presence or absence of security notices on Web sites.** (Advisory Committee Report at 15). Many sites may actually provide security, yet not inform consumers that they do so. The Commission majority's Report notes that security disclosures can enhance consumer confidence and are essential to informed consumer choice. (PR at 33 n.192). Indeed, "security notices are ineffective standing alone." (Advisory Committee Report at 21). Why, then, should the Privacy Survey's results measuring the frequency of security disclosures — not whether security is actually provided — be given any weight in assessing the progress of self-regulation of privacy online?

Security disclosures, particularly regarding the security of credit card information, might help increase consumer confidence. Yet this is a far cry from legislatively mandating the provision of "reasonable security" by Web sites and asking regulators to decide later what security is and is not "reasonable." The honest companies will provide security to satisfy their customers; the dishonest ones will simply not comply. There was no agreement among the

Advisory Committee members that the government should mandate security standards or that the Commission should be setting security standards.[22]

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." *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 758-59 (1985) (plurality opinion); *Trans Union Corp.*, 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

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

governmental interest asserted; and (4) whether the regulation is narrowly drawn to advance the governmental interest asserted. *Central Hudson Gas & Electric Corp. v. Public Serv. Comm'n of New York*, 447 U.S. 557, 561-63 (1980).

The Privacy Report provides no analysis of whether the governmental restrictions that it recommends would survive judicial scrutiny under the test articulated in *Central Hudson* and its progeny. It articulates no reasoned and documented basis for the conclusion that the recommended restrictions would directly and materially advance the governmental interest in protecting the privacy of consumers. Moreover, the Privacy Report presents no basis for the conclusion that the recommended restrictions are narrowly drawn to protect such privacy. Indeed, the Report does not present any information as to whether alternative legislation — for example, providing for Notice only — would protect the privacy of consumers yet impose a lesser burden on the exercise of commercial speech. In my view, we should not recommend that the Congress impose restrictions on commercial speech without conducting the necessary legal and factual analysis to state with confidence that the restrictions would survive judicial review.

7. Enforcement

It boggles the imagination to think about how the comprehensive regulatory scheme envisioned by the majority might be enforced. By enacting the broad statutory requirements recommended by the majority, Congress will create a new universe of law violators, most of whom are arguably innocent of harming consumers or other wrongdoing. Remember that **all** consumer-oriented commercial Web sites would be required to comply with the four FIPPs as implemented by government regulation.

Although a majority of the Commission suggests that self-regulation will continue to play a role in enforcement — perhaps through a mechanism like the dispute resolution and referral process of the National Advertising Division of the Council of Better Business Bureaus (PR at 36 n.202) — what is glaringly absent from the majority's recommendation is any type of safe

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

use a particular Web site or to seek an alternative.

The current recommendation, however, defies not just logic but also fundamental principles of governance. In recognition of some of the complexities of regulating privacy — particularly Access and Security — the Commission asks Congress to require all commercial consumer-oriented Web sites to comply with extensive, yet vaguely phrased, privacy requirements and to give the Commission (or some other agency) a blank check to resolve the difficult policy issues later. This would constitute a troubling devolution of power from our elected officials to unelected bureaucrats.

I dissent.

LIST OF HEADINGS

III. WHAT DOES THE REPORT FAIL TO DO?

A. The Report Does Not Adequately Credit Self-Regulatory Efforts

B. The Report Ignores Developments in Technology

C. The Report Fails to Identify and Consider the Costs and Benefits of Proposed Legislation

1. ***Notice***
2. ***Choice***
3. ***Access***
4. ***Security***
5. ***Competitive Effects***
6. ***Constitutional Issues***
7. ***Enforcement***
8. ***Offline Privacy***

IV. WHERE DO WE GO FROM HERE?