Comments of the Consumer Federation of America

to the U.S. Department of Commerce

Internet Policy Task Force

Docket No. 101214614-0614-01, RIN 0660-XA22

Information Privacy and Innovation in the Internet Economy

January 28, 2011

The Consumer Federation of America (CFA) is an association of some 300 nonprofit consumer organizations across the United States. Established in 1968, CFA's mission is to advance the consumer interest through research, advocacy and education. Consumer privacy is an important concern for CFA, especially since technology has fundamentally changed the ways that information about individuals can be collected and used, in many cases without their knowledge. CFA agrees with the statement in the Introduction to the new Department of Commerce (DOC) report, *Commercial Data and Innovation in the Internet Economy: A Dynamic Policy Framework* (hereinafter referred to as the green paper), that "Strong commercial data privacy protections are critical to ensuring that the Internet fulfills its social and economic potential."[1] But we believe that the report misses the mark in how it characterizes the current state of consumer privacy and in its recommendations for how to strengthen it.

This difference in perspective may be due, to some degree, to the fact that the DOC is not a consumer protection agency. Its mandate is to "advance economic growth and jobs" and its main function is to promote business interests here and abroad. We do not mean this in a pejorative way; that is a valid mandate, and it is clear that the DOC recognizes the importance of consumer trust in the growth of the Internet economy. The DOC has an important role to play in helping to inform U.S. privacy policy and in encouraging U.S. businesses to act responsibly. In these comments we will provide suggestions for how to address the urgent need to improve consumer privacy protection. Because the DOC has limited its focus to online privacy, we shall do so as well, but we note that protecting consumers' privacy offline is also critically important, and that as offline and online data are increasing melded, the differences between them are also becoming less distinct.

[1] See www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf at vi.

The problem is one of market failure.

Throughout the green paper there are statements about the current state of privacy protection in the United States that we do not believe are supportable, e.g. from the Foreword: “Our laws and policies, backed by strong enforcement, provide effective commercial data privacy protections.”[2] In fact, we have very few privacy laws, and contrary to the assertion in the Foreword, these laws do create a fragmented patchwork of protection, covering only specific entities such as financial institutions[3] and health care providers,[4] or very narrow situations such as the passing of consumers’ financial account number for marketing purposes from one company with which consumers have done business online to another online vendor[5] or sharing children’s online data.[6] We have the Federal Trade Commission’s (FTC) Self-Regulatory Principles for Online Behavioral Advertising[7] and voluntary industry self-regulatory programs which have proven inadequate to ensure that consumers have real control over the collection and use of their data. If the current regime was effective, there would be no reason to do more.

In its recent staff report, *Protecting Consumer Privacy in an Era of Rapid* Change (hereinafter referred to as the FTC report),[8] the FTC describes the underlying causes of the failure of the digital marketplace to create an effective regime for consumers to protect their privacy. This analysis must be the starting point for an effort to design a regulatory regime in the area of information flow that will be subject to ongoing regulatory oversight.

We created Table 1 to illustrate that the market imperfections leading to the failure of the market to protect consumer privacy are pervasive. The Table identifies five different types of market failure that appear to affect the gathering and use of information in cyberspace, each of which tends to undermine privacy. The general categories of market failure have been developed by CFA based on a review of the general academic literature as well as analysis of individual markets.[9] Using them to reflect the FTC’s analysis of the market failure demonstrates a pervasive, multifaceted problem.

---

[2] *Id.*at iii

[3] Gramm-Leach-Bliley Act., Title V of the Financial Servcies Modernization Act of 1999

[4] Health Insurance Portability and Accountability Act of 1996

[5] Restore Online Shoppers’ Confidence Act of 2010

[6] Children’s Online Privacy Act of 1998

[7] See www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[8] See www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[9] See Appendix A, *A Broad Framework for Analyzing Market Failure*

TABLE 1:
MARKET IMPERFECTIONS LEADING TO THE FAILURE OF PRIVACY PROTECTION IN CYBERSPACE

Societal: Situations where important values are not well reflected in market transactions

Externalities: Trust is undermined[1]

Non-economic Values: Concern,[2] Fear of Being Monitored,[3] and Exposed,[4] Reputational Harm,[5] Unwanted Intrusion,[6] Physical Security,[7]

Structural: Conditions that result in inefficient outcomes

Insufficient Competition: Incomprehensible Privacy Policies,[8] Inadequate Choice[9]

Economic Harm: Bad Purchase Decisions,[10] Security Breaches,[11] Identity theft [12]

Endemic: Tendencies of economic relations that undermine key market functions

Perverse Incentives: Incomprehensible Privacy Policies,[13] Slow to React[14]

Asymmetric Information: Speed of Technological Change[15] v. Slowness to React,[16] Difficulty of Detecting Harm,[17]Invisibility of Transactions and 3rd Party Relations[18]

Transaction costs: Frictions that impose costs and constrain exchange

Search and Information Costs: Lack of Simple and Clear Information,[19] Cost of Interrupting Transactions to Find, Evaluate and Act to Protect Privacy,[20] Invisibility of Transactions and 3rd party Relations to Consumers[21]

Bargaining Costs: Lack of Alternatives,[22] Inability to Define[23]

Policing and Enforcement Costs: Difficulty of Detecting Harm,[24] Complexity, Level and Amount of Information Gathered,[25] Rapid Pace of Technological Change,[26] Third Party Relationships[27]

Behavioral: Psychological and other human traits that bound "maximizing" actions

Motivation: Concerns,[28] Fear of Being Monitored[29]

Perception: Reputational Harm [30]

Calculation: Failure to Understand,[31] Failure to Appreciate Risk,[32] Lack of Awareness[33]

Execution: Struggle to Keep Pace,[34] Do Not Read[35]

Sources and Notes:

1. DOC, pp. vi, 1, 13, 15.
2. FTC, pp. iii, 28-30, DOC, pp. 3, 16-17.
3. FTC, p. iii.
4. FTC, p. 20.
5. FTC, p. iii.
6. FTC, p. iii.
7. FTC, p. iii.
8. FTC, pp. iii, 26..
9. FTC, p. 19.
10. DOC, p.1.
11. DOC, p. iii.
12. DOC, p. 1,
13. FTC, pp. iii, 26.
14. FTC, p. iii, DOC, p. 1.
15. FTC, p. 36.
16. FTC, p. iii.
17. FTC, p. 33.
18. FTC, pp. I, iii, 26.
19. DOC, p. vii
20. FTC, p. 27
21. FTC, pp. iii, 26.
22. FTC, p. iii.
23. FTC, p. iv, 35,
24. FTC, p. 33.
25. FTC, pp. ii, DOC, p. 18-19.
26. FTC, pp. ii, iii.
27. FTC, pp. ii, DOC, p. 16.
28. FTC, pp. iii, 28-30, DOC, pp. 3, 16-17.
29. FTC, p. iii.
30. FTC, p. iii.
31. FTC, p. ii, 26,, DOC p. 4.
32. FTC, p. ii.
33. FTC, p. ii.
34. FTC, pp. ii, 26.
35. FTC, p. iii.

The pervasiveness and nature of the market imperfections lead us to conclude that much more than transparency is necessary to correct the failure of the market to provide adequate privacy protection. The relationships between information gatherers and the technology of information gathering and exploitation make it highly unlikely that consumers will be able to keep up with and evaluate information on a real-time basis. Even where they have the skills and abilities, the transaction costs of doing so on a transaction-by-transaction basis would be very high.

As we describe in more detail later, we believe that a universal "Do Not Track" option is ideally suited to this marketplace. It affords those consumers who do not want data to be collected to opt out in a simple and across the board approach. To the extent that individual consumers want to opt in to specific types of data gathering, the "Do Not Track" approach can accommodate this.

The solutions must include limits on data collection and use and effective consumer control.

The green paper seems to suggest that the way to address concerns about online data privacy is to make information about data use more transparent and increase consumer understanding about the benefits of such uses. We have no quarrel with improving transparency or consumer understanding. In our recent report about consumer protection in cloud computing, we state that "Transparency is a

bedrock approach consumer protection challenges" and offer a model disclosure form.[10]

We also agree with the DOC that a clear notice is not always enough if it is insufficiently specific: "An entity that clearly states that it intends to do anything and everything with the data it collects may be transparent, but it may not be providing adequate protection for consumer privacy."[11] But as we said earlier, better transparency is not enough. Furthermore, the discussion in the green paper about the misalignment of consumer expectations and actual information practices misses a major point – that sometimes information practices, even if they are spelled out in detail and followed to the letter, are contrary to what consumers want or to the parameters that public policy sets to protect consumers.

Nowhere in the green paper, for instance, is there any discussion about whether consumers' health conditions, financial situations, sexuality, political activities, locations or other sensitive information should be off-limits for collection if not needed for a transaction that the consumer has initiated, or should require a heightened degree of consumer control. The green paper also neglects to ask whether some information should not be used for certain purposes. For example, is it appropriate to use information about who someone's friends on social networking sites are as a factor in determining the person's creditworthiness?[12] Should data about consumers collected online be used to determine their insurance risk?[13] There is also no real discussion about consumer choice – when is it needed, how choice should be obtained in various situations, whether there are some circumstances in which it is unfair to present data practices to consumers as "take it or leave it."

The FTC report examines these and other issues in detail, building on the record and knowledge base that the agency has assembled in exploring privacy for more than a decade and asking for further input. While there are some common ideas in the DOC green paper and the FTC report – for example, that privacy should be considered in the design and implementation of products and services (what the DOC calls "privacy impact assessments," or PIAs) – in many respects the approaches to solutions taken

---

[10] See *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, November 2010, http://www.consumerfed.org/pdfs/Cloud-report-2010.pdf.

[11] See green paper at 38.

[12] See Emily Steel and Julia Angwin, *On The Web's Cutting Edge, Anonymity in Name Only*, Wall Street Journal, August 4, 2010, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html, for a description of how online behavioral tracking is used to make assumptions about consumers to serve different credit card offers to them. See also Erica Sandberg, *Social networking: Your key to easy credit?*, January 13, 2010, http://www.creditcards.com/credit-card-news/social-networking-social-graphs-credit-1282.php.

[13] See Leslie Scism and Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, Wall Street Journal, November 19, 2010, http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html.

by the two agencies do not seem to be in sync at all. Again, this may be explained by the fact that consumer protection is not the core function of the DOC, as it is with the FTC.

The DOC can encourage solutions such as "Do Not Track" mechanisms by endorsing them and supporting legislation to enforce consumers' "Do Not Track" rights.

The concept of a persistent, universal "Do Not Track" mechanism to give consumers control over online behavioral tracking, which CFA strongly supports, is mentioned only briefly in the green paper and the DOC makes no recommendation in that regard. We believe that voluntary efforts by industry fall short of providing easy-to- find, easy-to-use, and effective tools for consumers who do not wish to be tracked online.

The National Advertising Initiative, which has offered an opt-out cookie for online profiling since 2000, is woefully inadequate because consumers do not know about it, there is no requirement that companies engaged in online tracking participate in the program (and some major players do not), there is no oversight or transparency, and there is no enforcement. Furthermore, opt-out cookies do not work for some methods of tracking and fail to provide persistent protection from unwanted tracking since cookies may be deleted for a variety of reasons.[14]

In July 2009, four trade associations jointly proposed voluntary principles[15] for online tracking, which included providing "choice" mechanisms for consumers. The principles contain many exceptions – for instance, no choice need be given for tracking by the website that the consumer is visiting or its affiliates. While the proposal calls for creating a centralized choice mechanism, which has only recently become available, companies that subscribe to the principles do not have to use it; they can provide their own choice mechanisms instead if they wish. It is also envisioned that there may be multiple self-regulatory programs in connection with the principles. While it is too early to assess the effectiveness of the principles or the choice mechanisms offered under this initiative, we believe that this approach is likely to be very confusing for consumers and to suffer from the same drawbacks as the NAI program: participation is voluntary, with no real oversight or enforcement, and the choice mechanisms will probably be based on cookies.

There are some positive aspects of the proposal by the four trade associations. One is the development of an icon that companies can use to indicate that online tracking is taking place. To the extent that a standardized icon becomes widely used and familiar to consumers, this may be helpful in

---

[14] See World Privacy Forum report, *National Advertising Initiative: Failing at Consumer Protection and at Self Regulation*, November 2007, http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.
[15] See www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209.

making tracking more visible. However, consumers may get the wrong impression if they do not see the icon – it will not mean necessarily mean that that tracking is not taking place, since using the icon is voluntary. In any case, self-regulatory programs can be a useful complement to legal requirements and prohibitions, but not a substitute.

Just recently Microsoft, Mozilla and Google have announced that their browsers will have new features to provide or facilitate "Do Not Track" solutions. Why have they done this? It is no coincidence that this occurred shortly after the release of the FTC report, in which the staff expressed its support for the concept of a universal "Do Not Track" mechanism.[16] Members of Congress are also talking about "Do Not Track."[17] It's a solution that clearly resonates with consumers; a poll commissioned last year by the nonprofit organization Consumer Watchdog in July 2010 revealed that 90 percent of Americans wanted more laws to protect privacy, 86 percent favored the creation of an "anonymous button" that allows individuals to stop anyone from tracking their online searches or purchases, and 80 percent wanted a "do-not-track-me" list for online companies that would be administered by the FTC.[18]

In order for a "Do Not Track" mechanism to work well for consumers, the FTC report recommends that must be an enforceable requirement for websites to honor consumers' "Do Not Track" requests. While the FTC has not called for legislation at this point, we hope that it will do so when it issues its final policy framework. The DOC should also support "Do Not Track" legislation. Just as consumers have the right to tell telemarketers not to call them and to opt-out of email solicitations, so should they have the right to opt out of online tracking when and if they wish. A "Do Not Track" mechanism can be flexible from both a technical and a regulatory standpoint. It can be designed to block any data from being collected about consumers' online activities or allow some data to be collected but not other data. This is the type of technological innovation that the DOC should vigorously promote.

---

[16] The FTC report said that given the limitations of opt-out cookies, the fact that an effective opt-out mechanism has not been implemented on an industry-wide basis, the lack of clarity about whether existing mechanisms prevent consumers from being tracked or simply prevent them from receiving targeted advertising, and the fact that consumers are not likely to be aware of the technical limitations of existing mechanisms, "Commission staff supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as "Do Not Track." See www.ftc.gov/os/2010/12/101201privacyreport.pdf at 66.

[17] See testimony of Susan Grant, CFA Director of Consumer Protection, before the House Committee on Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection, December 2, 2010, http://www.consumerfed.org/pdfs/Do%20Not%20Track%20Testimony%20of%20Susan%20Grant.pdf

[18] Seehttp://insidegoogle.com/wp-content/uploads/2010/07/wfreInternet.release1.pdf.

Voluntary codes of conduct are not, by themselves, enough to provide consumers with adequate privacy protection.

The DOC's proposed privacy framework endorses "voluntary enforceable industry codes" that are in line with Fair Information Practice Principles (FIPPs) and which would create safe harbors for companies. In our view, "voluntary enforceable industry codes" is an oxymoronic set of adjectives; a regime of privacy protection cannot be both voluntary and enforceable.

While we have no problem with looking to the FIPPs as a helpful set of principles – in fact, we refer to them in the Legislative Primer for Online Behavioral Tracking and Targeting[19] that CFA and several other consumer and privacy groups released in 2009 – we do not believe that there is any evidence that voluntary codes of conduct are enough, by themselves, to provide consumers with adequate privacy protection. We would also like to note that the FIPPs are high-level principles and do not completely address all concerns about online privacy. They do not, for instance, address whether collecting or using certain consumer data should be prohibited as a matter of public policy.

The DOC points to the U.S.-EU Safe Harbor Framework for the cross-border flow of information as an example of a successful self-regulatory effort, but it provides no evidence to substantiate that claim. A recent report[20] by the World Privacy Forum about the DOC's international privacy activities excoriates the U.S.-EU Safe Harbor Framework as being largely ineffective because of the failure to ensure that all companies that should be in the program are, that companies' claims to be participating in the program are valid, and that participating companies are actually complying with the program requirements. As we noted before, another self-regulatory program touted by the DOC, the National Advertising Initiative, has been a dismal failure, and the more recently announced voluntary self-regulatory programs for online behavioral advertising also have inherent shortcomings.

In 2003 when the FTC amended the Telemarketing Sales Rule[21] to create the national "Do Not Call" registry, the agency acknowledged that industry self-regulatory programs such as the Direct Marketing Association's Telephone Preference Service did not adequately protect consumers from unwanted telemarketing solicitations because these programs were voluntary and, "to the extent that

[19] See www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf.
[20] See *The US Department of Commerce and International Privacy Activities: Indifference and Neglect*, World Privacy Forum, November 2010, http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf.
[21] 16 CFR Part 310

sanctions exist for non-compliance, DMA may apply those sanctions only against its members, not non-members."[22]

The DOC attempts to address the inherent shortcomings of self-regulatory programs by proposing that a voluntary code of conduct for online privacy would be approved by the FTC. We believe that government approval of self-regulatory programs is only appropriate when there are already strong laws or regulations in place and the programs, based on rigorous criteria, are designed to provide consumers with protections and benefits beyond what the law requires. This was the approach taken by the Office of Fair Trading (OFT) in the United Kingdom in launching a Consumer Codes Approval Scheme, in which self-regulatory codes that meet certain criteria set by the OFT receive a government "seal of approval" in a two-stage process that requires the programs to demonstrate that they actually work.[23] The criteria include independent auditing and other checks to ensure that the programs do what they claim to do. The OFT makes clear that self-regulatory programs do not take the place of laws or regulations and that their main function is to enhance the consumer experience by encouraging, for instance, excellence in customer service.

The problem with online privacy is that there are *not* already laws in place here in the U.S. to provide strong and enforceable consumer protection. It is not possible to fill this vacuum with self-regulatory programs. Participation is voluntary, and enforcement consists of admonishing or ejecting the member. These programs give consumers no enforceable rights.

A narrow safe harbor, as part of privacy legislation, might be appropriate for well-delineated practices that are unlikely to cause consumers concerns. Both the FTC and the DOC have cited some practices that could merit safe harbor consideration. For instance, requirements for consumer consent may not be necessary when their data is used to fulfill their orders, for fraud prevention, and for other purely operational purposes (though those purposes need to be specifically outlined). We proposed in our Legislative Primer that perhaps consent would not be necessary for non-sensitive data that was only used for 24 hours.[24] It might also be appropriate to create a safe harbor that would exempt companies from having to provide consumers with access to their data if the data was kept for a very short time. But safe harbors should not be used to exempt companies from requirements such as for choice when those requirements are necessary to address privacy concerns.

---

[22] Federal Register Vol. 68 No. 19, January 29, 2003, at 4631.

[23] See information at www.oft.gov.uk/business-advice/business-codes/

[24] See http://www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf at 8.

U.S. consumers and companies need comprehensive privacy legislation to set the rules of the road.

The DOC asks whether baseline commercial data principles should be enacted by statute. We are not sure what the DOC means by "baseline," but something minimal, such as a codification of the FIPPs, which would be fleshed out by voluntary "best practices," is not sufficient. We have already noted that the FIPPs are high level principles and that do not cover all privacy concerns. Merely putting the FIPPs into law does not provide enough direction to either consumers or businesses about their rights and responsibilities. Putting meat on the bone through a stakeholder process that would lead to voluntary self-regulatory programs is not sufficient, either. The FTC, as the lead federal consumer protection agency, should be mandated to promulgate regulations that provide clear guidance to consumers and businesses about when choice is required, how choice should be obtained in specific situations, when consumer should be allowed to be shared with affiliates, what types of consumer data and uses of consumer data should be off-limits, what access consumers should have to their data, and other requirements and prohibitions as appropriate.

The FTC should remain the lead federal agency for developing U.S. policy concerning consumer privacy, for enforcement, and for consumer education.

It is important to recognize that the issue before us is not the exchange of business-to-business data, which raises its own set of privacy and security concerns. We are talking about *consumer* data. Consumer protection is a core mission of the FTC, and it is on that basis that the FTC has spent more than a decade exploring privacy issues and formulating policy responses. The complaints that the FTC receives and the investigations that it conducts help to inform that policy development. There is no other independent federal agency – and independence is a crucial factor when so many vested interests are involved – that is as well -placed as the FTC to play the lead role in developing U.S. policy concerning consumer privacy. We note that the FTC was recently admitted as a full member of the International Conference of Data Protection and Privacy Commissioners.[25] The FTC is the nearest thing to an independent federal data protection authority that we have in the United States. The FTC also has a strong consumer education mission – a mission that is not part of the DOC 's remit. In fact, there does not appear to be any section of the DOC Web site that provides educational information for consumers .

[25] See http://www.privacyconference2010.org/news_view.asp?id=24

Obviously, the FTC's enforcement authority is also important. Crucial to the FTC's policymaking and enforcement is its capability to promulgate regulations. The FTC needs Administrative Procedures Act rulemaking ability in order to respond to market failures in a timely manner, and it needs to have the ability to levy civil penalties.

The DOC has a very important role in advising the U.S. administration on telecommunications and Internet policy and in helping businesses understand their rights and responsibilities. The DOC and the FTC should work closely together on privacy policy and business education.

Others can play crucial roles in privacy protection enforcement.

States can use enforce consumers' privacy rights through their general statutes against unfair and deceptive acts and practices and specific state privacy laws and regulations. They can also be empowered to enforce federal laws. Private rights of action also play a crucial role in enforcing consumers' right and changing company behavior. Government agencies do not have the resources to pursue every case that may merit formal legal action. Companies can also help to enforce consumers' privacy rights by ensuring that their contractors comply with legal requirements and other standards, and by alerting law enforcement authorities to problems that they may see in the marketplace.

The DOC should not create a Privacy Policy Office.

The DOC does not need to expend resources on creating a new Privacy Policy Office in order to coordinate work on commercial data privacy internally; the green paper shows that the DOC is already fully capable of such coordination. Nor is there any impediment to convening stakeholders meetings under the current DOC structure.

Moreover, we are concerned that the creation of a Privacy Policy Office at DOC might be interpreted by some as an attempt to usurp the FTC in the development of policies to protect consumer privacy and undercut the agency's effectiveness . Businesses should not be able to "forum shop" for the privacy frameworks that they feel are most favorable to them.

The role of a stakeholders group should be to provide input to the DOC, not to set policy or devise best practices.

It might be useful for the DOC to convene a diverse group of stakeholders to discuss consumer privacy. The green paper was developed with very little input from consumer or privacy advocates. That is not the DOC's fault – CFA and many other groups were simply unable to respond at the time, and our

absence shows in the record, which overwhelmingly reflects business views. Therefore, the green paper is incomplete as a compendium of the full range of views on the subject of online privacy. A stakeholders group can help supplement that record and keep the discussion moving. As with industry, the consumer and privacy community is not monolithic, and it would be best to have perspectives from as many consumer and privacy advocacy representatives as possible. The composition of a stakeholders group must be fairly balanced.

CFA has long experience in convening stakeholders groups and participating in groups convened by others. We know that in the contentious area of consumer privacy, there is likely to be very little consensus about the best solutions to privacy concerns or how to attain them. We do not believe that a stakeholders group could reach agreement on a comprehensive and sufficiently strong set of best practices, and we are not sure how much value such a process would have without legal privacy protections to underlie it. As we noted before, best practices should encourage companies to go beyond the law, and we do not have the legal underpinnings. Furthermore, it is the not the proper role of a stakeholders group to make DOC policy; its role should only be advisory in nature.

A national breach notification law should not preempt the state from providing better protection for their constituents.

According to the National Conference of State Legislatures, as of October 2010 forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands had data breach notification laws.[26] The states acted, as they have a right and an obligation to do, to fill the vacuum left by inaction on the federal level. We understand the concern about the lack of legal uniformity, though we would point out that technology helps to facilitate compliance with differing state laws. While it we agree that it would be good to provide consumers with breach notification rights in states that do not have them, the price of doing so would be too high if it resulted in significantly weakening the rights that consumers in states that do already have.

One key concern is whether federal legislation would impose a “risk of harm” trigger. In the best state laws, such as those in California, Texas, New York, and Illinois, notice is required when specific sensitive information is the subject of a breach, without any determination as to whether consumers might be harmed, which may be difficult to foresee.

[26] See http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx.

CFA generally opposes state preemption.

As a general matter, CFA is opposed to preempting state consumer protection laws because states are often the first to identify problems in which consumer protections are needed and the quickest to enact such protections. Often good ideas that are first implemented at the state level are eventually adopted at the federal level. For example, the California Legislature passed a law in 2001 (SB 125) to enable victims of identity theft to obtain documentation held by credit card companies and other financial institutions, such as the fraudulent credit applications submitted by their impostors. Prior to this law, many victims had difficulty obtaining the very documentation they needed to prove they were indeed being impersonated. This important provision was inserted into the federal FACT Act and is now law across the land.[27]

Conclusion

CFA appreciates the opportunity to provide these comments to the DOC. Since time constraints limit the issues we can address in our comments, we have joined with other consumer and privacy groups on separate comments concerning the online privacy of children. CFA is committed to working with the DOC and other federal agencies to create a framework for privacy that provides strong protection for consumers and certainty for businesses.

[27] Fair and Accurate Credit Transaction Act of 2003, FCRA § 609(e)

Appendix A

A Broad Framework for Analyzing Market Failure[28]

The Traditional Approach: Externalities and Structure

Market failure is a sufficiently widespread phenomenon to be recognized as an important analytic issue even for introductory economic texts. In one widely used text, John Taylor states that "in certain circumstances – called market failure – the market economy does not provide good enough answers to the "what, how and for whom" questions, and the government has a role to play in improving on the market"[29] Taylor defines market failure as "any situation in which the market does not lead to an efficient economic outcome in which there is a potential role for government."[30] Taylor identifies the "major sources of market failure as "public goods, externalities, and monopoly power."[31]

An advanced text on antitrust and regulation offers the following observation on the importance of market failure in economic analysis:

> If we existed in a world that functioned in accordance with the perfect competition paradigm, there would be little need for antitrust policies and other regulatory efforts. All markets would consist of a large number of sellers of a product and consumers would be fully informed of the product's implications. Moreover, there would be no externalities present in this idealized economy, as all effects would be internalized by the buyers and sellers of a particular product.
>
> Unfortunately, economic reality seldom adheres closely to the textbook model of perfect competition. Many industries are dominated by a small number of large firms. In some instances, principally the public utilities, there may be a monopoly. Consumers who use hazardous products and workers who accept risky employment may not fully understand the consequences of their actions. There are also widespread externalities that affect the air we breathe, the water we drink, and the future viability of the planet.[32]

These citations identify three broad areas of analysis that are common in the literature:

- structural conditions of supply, e.g. lack of competition (small numbers or monopoly);
- consumer behavior, e.g. ill-informed or unaware, and
- societal, e.g. externalities and products (public goods)

---

28 Excerpted and updated from: Mark Cooper and Barbara Roper, *Reform of Financial Markets: The Collapse of Market Fundamentalism and the First Steps to Revitalize the Economy* (Consumer Federation of America, March 2009); *Comments of the Consumer Federation of America, Rulemaking to Establish Light-Duty Vehicle Greenhouse Gas Emission Standards and Corporate Average Fuel Economy Standards,* November 27, 2009.

29 John B. Taylor, *Economics* New York: Houghton Mifflin, 1998), p. 49.

30 Taylor, Economics, p. 405.

31 Taylor, *Economics,* p. 404.

32 W. Kip Vsicusi, John M. Vernon and Joseph E. Harrington, Jr., *Economics of Regulation and Antitrust,* Cambridge: MIT Press, 2001), p. 2.

Over the past several decades criticism or and refinements to the traditional economic model have expanded the analysis of factors that cause markets to fail to arrive at outcomes that have traditionally been defined as efficient.[33] This broader perspective is presented in Figure A-1. The major categories are discussed briefly below, with greatest attention to the newer categories.

Societal

The societal category refers to situations in which important values are not reflected in market transactions. The traditional example is externalities.[34] However, the category should be expanded to include network effects, which are sometimes referred to as network externalities,[35] innovation economics,[36] and the general proposition that non-economic values are often the drivers of human activity. It can be argued that the importance of innovation economics derives significant support from the new institutional economics and the importance of non-economic values derives significant support from behavioral economics.

Endemic

Some of the problems that have long been recognized in traditional economics and could be located within the structural category involve such fundamental assumptions about the functioning of markets that are so frequently violated they rise to the level of endemic problems. Here, too, it can be argued that new institutional and behavioral economics support the proposition that these flaws deserve special attention. Joseph Stiglitz, Nobel Laureate, Chairman of the Council of Economic Advisors and Chief Economist at the World Bank, identified the threat problem that these flaws pose in the financial sector well before the financial meltdown.

> Joseph E. Stiglitz, The Roaring Nineties: A New History of the World's Most Prosperous Decade (New York: W.W. Norton, 2003)
>
> **Conflicts of Interest** "Deregulation enhanced the scope for conflicts of interest. It also had the advertised effect of increasing competition. In normal circumstances, increased competition is a good thing. But in the nineties, the banks became so eager for short-term profit that here was a race to the bottom. Each bank knew that

FIGURE A-1: COMPREHENSIVE LIST OF IMPERFECTIONS THAT CAUSE MARKETS TO FAIL

---

[33] A constructive view is taken by leading behavioral economists (amerer, Colin, F. and George Lowensetin, "Behavioral Economics: Past, Present, Future," in Colin f. Camerer, George Loewenstein and Matthew Rabin (Eds.), *Advances in Behavior economics* (New York: Russel Sage foundation, 2004), p. 3: "This conviction does not imply a wholesale rejection of the neoclassical approach to economics based on utility maximization, equilibrium, and efficiency. The neoclassical approach is useful because it provides economists with a theoretical framework that can be applied to almost any form of economic (and even noneconomic) behavior, and it makes refutable predictions. Many of these predictions are tested in the chapters of this book, and rejections of those predictions suggest new theories.

[34] Taylor, p. defines an externality as a "situation in which the costs of producing or the benefits of consuming a good spillover onto those who are neither producing nor consuming the good."

[35] "In economics and business, a **network effect** (also called **network externality** or **demand-side economies of scale**) is the effect that one user of a good or service has on the value of that product to other people. When network effect is present, the value of a product or service increases as more people use it." http://en.wikipedia.org/wiki/Network_effect

[36] Innovation economics is based on two fundamental tenets: that the central goal of economic policy should be to spur higher productivity and greater innovation, and that markets relying on price signals alone will not always be as effective as smart public-private partnerships in spurring higher productivity and greater innovation. http://en.wikipedia.org/wiki/Innovation_economics

TRADITIONAL AND INDUSTRIAL ORGANIZATION ECONOMICS

NEW INSTITUTIONAL AND BEHAVIORAL ECONOMICS

INDUSTRY STRUCTURE

Imperfect Competition
- Concentration
- Barriers to Entry
- Scale
- Vertical Leverage
- Collusion

ICE problems
- Price discrimination
- Entry barrier
- Bargaining

Technology
- R&D
- Investment

Marketing
- Bundling: Multi-attribute
- Product Differentiation
- Gold Plating
- Inseparability
- Purchase Method

SOCIETAL FLAWS

Traditional Externalities
- Positive
- Negative
- Public Goods
  - Basic research
  - Information
    - Learning-by-doing
    - Learning-by-using

Network Effects

POWER

Legal Framework
- Property
- Contract

Policy
- Taxation
- Subsidies

ENDEMIC IMPERFECTIONS

Asymmetric Information
- Agency
- Moral Hazard
- Adverse Selection

Perverse Incentives

Conflict of Interest

TRANSACTION COST

Search and Information
- Imperfect Information
  - Availability
  - Accuracy
  - Search Cost

Bargaining
- Risk & Uncertainty

BEHAVIORAL BASICS

Motivation Values & Commitment
- Bounded Selfishness/wants
  - Morality
  - Fairness/reciprocity
  - Altruism
  - Preference
  - Custom
  - Social group & status

Perception
- Bounded Vision/Attention
  - Prospect
    - Framing
    - Loss Avoidance
    - Status Quo
    - Salience

its competitors were engaging in similar practices, and if it did not compete, it would be left behind; and each banking officer knew what that meant; small bonuses, perhaps even being fired. (p.1 3)

Perverse Incentives: The CEOs and other executives of corporations are supposed to act in the best interests of the corporations, its shareholders and workers; but in the nineties, incentives got badly misaligned. In acting in their own interests, CEOs often did not serve well those on whose behalf they were supposed to be working. The irony was that the changes in pay structure which were at the root of much of the problem were defended as improving incentives... Investment houses became marketers…. They did what it took to sell what they could sell p. 149,

Asymmetric Information: For the stock market to function well, there needs to be accurate information about what a company is worth so that investors can pay the right price for its shares. By obfuscating the problems inherent in many of the companies they brought to the market or for which they helped raise capital by issuing shares, the banks contributed to the erosion of the quality of information. They were supposed to provide information to investors, to reduce the disparity between informed insiders and outsiders. Instead, asymmetries of information maintained or increased; in many cases, bankers and analysts knew the real state of affairs about the companies they worked with but the public did not. Confidence in the markets declined, and when the correct information came out, share prices declined sharply. (p. 141)

Transaction Costs and the New Institutional Economics

Transaction cost economics is framed as a critique of neoclassical economics. "The costliness of economic exchange distinguishes the transaction cost approach from the traditional theory economists have inherited from Adam Smith… An exchange process involving transaction costs suggests significant modifications in economic theory and very different implications for economic performance."[37] Transaction costs analysis launches from the observation that there is friction in human activity that is not accounted for in the neoclassical models of economic behavior. Failing to take transaction costs into account misrepresents the cost of action and therefore the pattern of activity that occurs. Noting the difference from neoclassical assumptions, Douglass North, one of the first to receive a Nobel Prize in this school of economics, argued as follows.

If political and economic markets were efficient (i.e., there were zero transaction costs) then the choices made would always be efficient. That is, actors would always possess true models or if they initially possessed incorrect models the information feedback would correct them. But that version of the rational actor model has imply led us astray. The actors frequently must act on incomplete information and process the information they do receive through mental constructs that can result in persistently inefficient paths….

The theory is based on the fundamental assumption of scarcity and hence

[37] Douglass C. North, *Institutions, Institutional Change and Economic Performance* (Cambridge: Cambridge University Press, 1990), p. 27.

.

competition; its harmonious implications come from its assumptions about a frictionless exchange process in which property rights are perfectly and costlessly specified and information is likewise costless to acquire. Although the scarcity and hence competition assumption has been robust and has provided key underpinnings of neoclassical theory, the other assumptions have not survived nearly so well.

For the past thirty years, other economists and other social scientists have been attempting to modify and refine the issue to see just what have been missing from the explanation. Put simply, what has been missing is an understanding of the nature of human cooperation and coordination.[38]

Information is the resource at the center of transaction cost and institutional economics because "the costliness of information is the key to the costs of transacting, which consists of the costs of measuring the valuable attributes of what is being exchanged and the costs of protecting rights and policing and enforcing agreements.[39]

Institutions are formed to manage and reduce transaction costs.

Institutions provide the structure for exchange that (together with the technology employed) determines the cost of transacting and the cost of transformation. How well institutions solve the problems of coordination and production is determined by the motivation of the players (their utility function), the complexity of the environment, and the ability of players to decipher and order the environment (measurement and enforcement).[40]

The creation of organizations may create inertia, lock in on inefficient solutions, or conflicts of interest that result in wide from the second best solution that the institutions are intended to achieve[41] The deviation of the institutions from their ideal is the result of the difficulty of enforcement, "there are two reasons why enforcement is typically imperfect… the cost of measuring the multiple margins that constitute contract performance [and] the fact that enforcement is undertaken by agents whose own utility functions influence outcomes."[42] Central to the challenge of monitoring, is the agency issue. "The agency issue is ubiquitous in hierarchical organizations. The problem of monitoring and metering the various attributes that constitutes the performance of agents in contrast to the standard neoclassical frictionless model.[43] Thus, agency, asymmetric information and conflicts of interests are the barriers and imperfections in that drive organizations farther from the goal of efficiency.

Behavioral Economics

Over the three decades, behavioral economics has sought to extend the traditional economic model by incorporating more realistic assumptions about human behavior.

[38] North, p8…. 11.
[39] North, p. 27.
[40] North, p. 34.
[41] North, p. 7.
[42] North, p. 54.
[43] North, p. 32.

> At the core of behavioral economic analysis is the conviction that increasing the realism of the psychological underpinnings of economic analysis will improve the field of economics *on its own terms* – generating theoretical insights, making better predictions of field phenomena, and suggesting better policy…
>
> For example, there is nothing in core neoclassical theory that specifies that people should not care about fairness, that they should weight risky outcomes in a linear fashion, or that they must discount the future exponentially at a constant rate. Other assumptions simply acknowledge human limits on computational power, will power, and self-interest.[44]

The neoclassical paradigm at the core of market structural analysis makes assumptions about the nature of human behavior that are necessary for its propositions and conclusions to be valid. Economic actors are presumed to be narrowly focused on their own economic interest and fully capable of pursuing those interests with rational precision. People are assumed to rationally and consistently pursue selfish, utility maximization according to a time consistent discounting model based on Bayesian probabilities for outcomes in which all income and assets are fungible.[45]

Behavioral economics challenges every assumption of this model of economic actors at the level of motivation, perception and calculation. For purposes of policy analysis, we believe the findings of behavioral economics can be usefully divided into four groups – motivation, perception, calculation and execution. Wilkinson's *Introduction to Behavioral Economic*, has two sets of chapters, one foundational, one advanced, that can be organized according to this scheme as follows:

---

[44] Camerer, Colin, F. and George Lowensetin, "Behavioral Economics: Past, Present, Future," in Colin f. Camerer, George Loewenstein and Matthew Rabin (Eds.), *Advances in Behavior economics*(New York: Russel Sage foundation, 2004), p. 3.

[45] Paraphrasing Wilkinson, Nick, *An Introduction to Behavioral Economics* (Hampshire, Palgrave, 2008); Camerer, Colin F, George Lowenstein and Matthew Rabin (Eds.), *Advances in Behavioral Economics* (New York: Russell Sage, 2004). Introduction, p. 5.