AMERICAN BAR ASSOCIATION

Section of Science & Technology Law
321 N. Clark Street
Chicago, IL 60654-7598
(312) 988-5599
FAX: (312) 988-6797
sciencetech@abanet.org
www.abanet.org/scitech

February 8, 2011

Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Comments in Response to FTC Request for Comments on the FTC's preliminary report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*

Dear Chairman Leibowitz:

We are writing on behalf of the American Bar Association Section of Science & Technology Law to provide comments on the FTC's preliminary report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers.*

The views expressed in the attached comments are those of the Section of Science & Technology Law. They have not been submitted to or approved by the ABA House of Delegates or Board of Governors, and should not be construed as views of the Association as a whole, although, as indicated in the comments, we have consulted with several other interested sections of the ABA. These comments are within the Section's primary and special expertise, and were approved by the Section Council on February 2, 2011.

The Sections appreciate the FTC request for input. If you have any questions or would wish further explanation for our comments, please feel free to contact me.

Very truly yours,

Stephen S. Wu, Chair
American Bar Association
Section of Science & Technology Law

Comments in Response to a Request for Input by the Federal Trade Commission (Bureau of Consumer Protection) on its Staff Report entitled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

The views expressed in the attached commentary are provided by the Section of Science & Technology Law of the American Bar Association ("ABA SciTech" or "SciTech"). These comments have not been submitted to or approved by the ABA House of Delegates or Board of Governors, and should not be construed as views of the ABA as a whole.

The views expressed herein represent comments intended to both protect the rights and interests of both business and consumers.

I. Introduction

This commentary is provided in response to a call from Federal Trade Commission (Bureau of Consumer Protection) (the "FTC") for public comment to the proposed report: *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (the "Report"). The Report provides a proposed framework for balancing the privacy interests of consumers with the interests of businesses when developing products and services through use and analysis of consumer information. These comments are intended to address, where possible, the specific questions posed by the FTC and reflect the general consensus of SciTech. We note, however, that many questions remain which were not asked but are central to any privacy framework. These include, for example, policy questions such as the type contained in the comments submitted by the ABA's Antitrust section, and more mundane but critical questions, such as how the FTC envisions defining "consumer" as used in the Report. The Report clearly envisions individuals acting primarily for personal, family or household purposes, but it is less clear whether it encompasses all individuals such as employees. If the Report is intended to cover all individuals, considerable additional comments will be necessary and appropriate.[1]

These comments are provided in support of the efforts and direction of the FTC's goals of a balanced approach toward consumer privacy protection, technological innovation, and healthy business practices. We sincerely appreciate the FTC's offering public comment to the Report, and look forward to collaborating and providing input on these critical issues of consumer privacy protection.

---

[1] For example, the Report appears to envision that use of data will automatically be dependent upon prior consumer consent after full disclosure, yet there are myriad, legitimate employment situations that cannot be envisioned at the onset of employment and for which consent will not be appropriate. Similarly, the Report seeks comment on "take it or leave it" situations – is that a request for comments on consents such as by "at will" employees or by existing employees with contracts for a set period (which contracts do not include clauses necessary to address issues created by a framework that did not exist when the contracts were signed)? Our comments in this letter assume that employees are not included as "consumers" under the framework. If that is incorrect, we respectfully request a new comment period to address same.

II. Comments

As noted throughout, SciTech supports the efforts of the FTC to promote the appropriate use and control of consumer information without stifling productive uses of the information in a responsible manner. SciTech appreciates the ability to comment on the Report and provide further context to some recommendations.

A. Scope

Are there practical considerations that support excluding certain types of companies or businesses from the framework – for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?

In line with the draft report, any consideration of Scope needs to be seen through the lens of at least the three overarching principles:

1. Context
2. Complexity
3. Harm[2]

The sensitivity of personal information is a function of its potential for causing harm to a person (such as the data subject, the collecting entity or others) and the importance a reasonable person would place on protecting it, neither of which is necessarily a function of the type of business collecting the information. Harm is also impacted by the context of the relationship, such as between a data subject and a business. Many businesses have both direct and indirect relationships with individual data subjects. Where there is a direct relationship, the business will have a different set of motivations as well as a different set of opportunities to influence the individual's choices around what and how data is collected, used, and disclosed, In an indirect relationship, such as those involving third parties or service providers, interactions – and legal frameworks – may be quite different. Even when contracts exist in such indirect situations, the parties will not necessarily be able to directly manage the environment to ensure compliance (e.g., a merchant attempting to require its bank to provide express data protection obligations for the merchant).

Due to the contextual nature of data protection, there are two primary modes by which the Report's framework can regulate appropriate privacy protections: (1) direct regulation on a "covered entity" and (2) indirect regulation by requiring any "covered entity" to pass on its obligations to any third party service provider via contract. As noted, however, this contractual route assumes leverage that may or may not exist and not all distribution structures will even accommodate such participant-by-participant contracts.

---

[2] Harm needs to be evaluated in the business, as well as the consumer, harm context. There are strong public policy reasons supporting the limited free flow of information without an individual's right to notice, choice, or access & correction. For example, the effectiveness of a credit reporting agency would be severely curtailed if an individual could force a CRA to replace accurate negative information on a credit report, with inaccurate positive information (under the guise of asserting access & correction rights). Other examples include, anti-fraud activities, police investigations, public safety management, land recording statutes, etc.

A fundamental component of the framework needs to be that the obligations agreed to at the point of collection carry forward with the data throughout its lifecycle. This way, inartful drafting of the framework will not subject businesses having no direct contact with a data subject to obligations which are appropriately managed by those businesses that do have such direct contact. The most obvious example of this is the service provider that the consumer never knows is present, who operates as an agent on behalf of the principal's business. It is the principal's privacy promises which are important to the individual data subject. Further, this allows the consumer, the data collector, and any third parties to have certainty about the processing, storing, and forwarding of data.

In addition, appropriate consideration should be given to the value companies have in maintaining and analyzing information about their clients and customers. A privacy-protective framework, and any collateral regulation, is justified to the degree that misuse or public disclosure of sensitive consumer information would cause harm to the individual, while not over-burdening business. As a result, such a framework should provide clear guidance to companies to promote both consumer protection and legitimate commercial uses and to provide certainty within the commercial marketplace. Not doing so would complicate businesses' implementation of appropriate privacy-protective controls and could lead to a chilling of legitimate commercial use, or worse, drive businesses to attempt to work around (rather than within) the framework.

Additionally, it is important that the FTC considers the complexities of the global privacy framework and take into account the globalized nature of U.S. business and analyze how a contemplated framework would fit within that context.

It is possible that in applying the concepts of context, complexity, and harm, it is reasonable not to apply some provisions of the framework to certain businesses. For example, some parts of the framework may not usefully apply to small businesses that continue to maintain substantial records in paper format. Also, some provisions may not usefully apply businesses that do not maintain a consumer-facing interactive electronic "storefront."

Is it feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device"?

This question involves more than feasibility. Any proposed framework looking to an expansion of the regulatory obligations needs further consideration of the legal basis for such legislative or regulatory exercise of authority.

With respect to the Report's question, however, there may be some confusion as to what kinds of data are included or whether data may become covered by the framework if it becomes "identifiable" information when linked with other data. For instance, would a database consisting of items purchased at a particular time fall into this "linkable" category? This information, by itself, hardly consists of personal information. However, if combined with security surveillance footage of cash registers or ATM machines, for example – something most people would not consider either personal or private information – any such data could be reasonably linked to a particular person. Both forms of information have legitimate business purposes and, when combined, can be reasonably linked to a specific consumer. There is also question as to the applicability of information that individuals either purposely publicize or knowingly make available to the public. This may include

information like a person's username a publicly accessible site, the IP address one is using to access the Internet, or information posted to a blog.

Where the framework applies to data that has actually been linked together, and where such linkage can then be used to identify a specific individual, then it is feasible for the framework to apply to such "linkable" data. However, in the absence of such actual linkage, such a framework would apply to any or all data. Such over-broad applicability to data which may never be actually linked, but has a potentiality of linkage, is not feasible and would impose significant and onerous costs on businesses that would eventually be passed on to consumers. Additional review of operational issues will also reveal a plethora of cases to the effect that consumers do not have a reasonable expectation of privacy in data provided to a third party not acting merely as an intermediary, which cases are also critical to the prevention of fraud and identity theft. What is or should be protected data under existing or future frameworks needs to be considered in light of the public policy balances inherent in such cases.

Additionally, using the term "specific consumer, computer, or other device" introduces some presumably unintended ambiguity as well. The FTC may should be concerned about a linkage between consumers and their devices (including computers), the scope of the proposed framework could be better drafted. We suggest that the FTC's apparent intent would be better reflected if the proposed framework were to apply to "data or collections of data that reasonably identify a specific person or specific device associated to a specific person." This phrasing captures both the linkage between specific persons and specific devices as well as the concern around usage of aggregated databases. Without the limiting phrase "associated to a specific person," transient usage of publicly accessible devices (such as usage of an informational kiosk at a museum or a ticket dispenser at subway station) would be included. It is doubtful that the FTC intends to include such transient moments within the scope of the proposed framework.

How should the framework apply to data that, while not currently considered "linkable," may become so in the future?

Are there reliable methods for determining whether a particular data set is "linkable" or may become "linkable"?

Given enough information, all information could be linkable. However, regulating all information as linkable would chill legitimate usage. If any "linking" concept is appropriate, it should be technology agnostic, but also defined and concrete enough so that companies know what is and is not linkable without needing to be savants regarding both existing and developing technologies. If any "linking" concept is appropriate, there should also be a requirement that the data be linked *before* a data protection is triggered – this would be to allow for the use of aggregated or anonymous data. Using this type of trigger also, from a practical perspective, may be necessary to allow compliance: data which is *not* considered PII when collected can become so when placed into another context (*e.g.* a relational database). Absent conditioning protection on actual linkage, compliance would appear to become a Catch-22. Even with such a condition, it may, in fact, be impossible for companies to know when they have created linked data (*e.g.*, company using a relational database that reasonably does not understand or anticipate all possible relations).

What techni cal measu res exist to "anon ymize" data and are any industry norms emerging in this area?

There is rapid innovation in the field of da ta m ining and data linkage, and it would be extremely di fficult to craft a legal framework at t his point when possibiliti es are either unknown, un tested, or highl y speculative. There are so me best practic es to ensure that sensitive information is anonymized in a manner appropriate for the particular use. However, due to the way anonymizing technology works, where a sufficiently large enough data set is put together, one may be able to reverse engineer an identity. This is why the appropriate test to determine if a data set should be protected isn't whether or not anonymizing technology has been applied to it, but if the data set itself can be used to identity a discrete individual.

As a gen eral matter, data intended for public disclosure or broad internal usage can be anonymized through (a) rem oval of all unique ly identify ing fields (such as name, social security or driver' s license num bers, and uni que account num bers) and (b) aggregation of data in sufficiently large sample sets. What constitutes a "sufficiently large sample set" will depend on t he nature of the data and the form of aggregation. For instance, a ggregated and anonymized data linking the cost of treat ment to a particular dise ase for a l arge urban are a may be valuable to the general public. However, if there is only one person in that sample set with a rare condition, this would hardly be anonymous, even when aggregated.

This kind of issue can be addressed thr ough a wide variety of technologies that would lim it the sample set used when creating such data. The examples of "re-identification" (with AOL and Netflix) cited in Secti on (IV)(B)(5) of the Report c onsist of anony mized but non-aggregated d ata. However, with the appropriate sized sa mple set, this com bination of aggregation and anony mization allows ne w dat a to be created, analy zed, processe d, monetized, and distrib uted without sa crificing consu mer privacy an d inclu de many of th e benefits discussed at the roundtables and addressed in Section (VI)(B)(4) of the Report. At its core, anon ymizing technolog y is just anothe r technolo gy whi ch may be deployed i n an effective or an ineffecti ve manner depending on the context and architecture of t he deployment.

B. <u>Consent</u>

The Commission could serve a useful role by considering what kinds and methods of consent are, or are n ot appropriate; and whether consu mers are benefite d in fact by the consent process. Cur rently, there are a wide array of channels through which information is both provided and collected, and the num ber of such channels are only increasing and broadening. By way of example, Americans sent and received 12.2 million text messages in June of 2000, 7.2 billion text messages in June of 2005, and 173.2 billion text messages in June of 2010. [3] Each new ch annel provides new chall enges in ac quiring t he appropriate con sumer consent. Technology has already r endered so me of the ex isting rules archaic, and try ing to squeeze those rules into new technologies m ay do m ore to irritate consumers than to benefit them . These issues are complex and would benefit from further notice and comment once the FTC can provide more specifics of the consent requirements and formats it envisions.

---

[3] http://www.ctia.org/consumer_info/service/index.cfm/AID/10323

With respect to commonly accepted practices that should not require consent, and in addition to our later comments on that topic, websites should be allowed to collect a certain amount of information merely by the consumer's act of accessing a site. This incidental information at least includes the HTTP header information (which includes some device specific information)[4], and other information necessary to maintain the security and integrity of the site. Some of this information may include information that either identifies a person or a device, or can be linked (depending on the definition) to a person or device. Formally requesting the information or permission to collect such incidental information may hinder the transaction, frustrate user experience, and undermine the integrity of a site's security. Requiring each business to implement such controls would have a similar effect. However, if browser providers embed technologies that allow consumers to make decisions about sharing their information – as many of them already have – then consumers would have a single point of control without having to rely on business-specific implementations. Its effectiveness would depend on how the browser interacts with each website that the user visits.

As the Report references in Section (IV)(B)(5), the roundtable discussions raised the claim of a decreasing relevance between some PII and non-PII, which can also affect when and how consumer action or access alone could be sufficient consent. Businesses may ask for information that is necessary and relevant to service a consumer or process a transaction (such as an email address for a service providing information only by email) and leave other information optional or not request it at all (such as a name or address). However, decisions by the consumer will cause businesses to incidentally collect personal information if, for instance, a person uses her name or address as part of her email address (email prefixes such as "JaneXSchmitt_Oct5" or "NYC_JoeRizzo_1975"). A consumer's choice to include sensitive information in what would otherwise be non-sensitive data may change the classification of a data in a way beyond the control of the business and, indeed, the business may be completely unaware that a consumer happened to have embedded identifying information in otherwise non-sensitive data. This incidental collection of information should not trigger new duties for the business.

What types of disclosures and consent mechanisms would be most effective to inform consumers about the trade-offs they make when they share their data in exchange for services?

Many consumer privacy policies and practices are provided in dense legal documents that may not be understandable or accessible to consumers. This is not necessarily avoidable, however. Some forms are legalistic because text reflects case law or statutory requirements of various states or countries, and "plain language" might not achieve the intended effect at all. Most policies are long because of FTC enforcement actions interpreting as deceptive statements that it determined were inaccurate or incomplete. Websites seeking to avoid a similar fate learned quickly that achieving accuracy takes details (length). As with the Model Financial Privacy Notice mentioned above, to the extent possible, perhaps the FTC could suggest model statements with model definitions reflecting typical realities. That might allow companies with "typical" data practices to use the pre-set language.

---

[4] http://www.w3.org/Protocols/rfc2616/rfc2616-sec5.html#sec5.3 or http://en.wikipedia.org/wiki/List_of_HTTP_header_fields.

C. "Privacy by Design"

Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced?

Section V(B)(1) provides that companies should incorporate substantive privacy protections into
their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy. Before answering the above question, it will be appropriate to ask questions that are not asked in the Report and to give considerably more consideration to assumptions and statements made in Section V(B)(1) over a much longer time period than the current comment period, even as extended. For example, this statement is made on page 47:

> Finally, companies should take reasonable steps to ensure the accuracy of the data they collect, particularly if such data could be used to deny consumers benefits or cause significant harm. For example, some data brokers sell identity verification services to various public and private entities. If the information is erroneous and does not match the identifying information a consumer presents to gain a benefit – such as accessing funds or services – the consumer can suffer economic or other harm.

This statement raises the question of what is public data, what uses may be made of it, including the consequences of "correcting" data from public records which always include inaccuracies. These may range, for example, from a deliberately erroneous weight on a driver's license to an address on a deed made inaccurate by time, but still relevant to issues pertaining to the deed or for verification via knowledge of previous addresses. The statement also creates issues not addressed by the questions asked in the Report.

For example, assuming that benefits are being denied such that consumers are suffering the alleged harms: are or should such services be regulated as consumer reporting agencies under the Fair Credit Reporting Act and what impact on the cost and ability to provide verification services would that have? Should users of such services be regulated as "users" of consumer reports under the FCRA? Should consumers be afforded FCRA correction rights when verification is at issue and a consumer identity thief will, by definition, seek to make inappropriate "corrections"? Should Congress, the author of FCRA, be the one to make these determinations and do so by legislation?

Is there a way to prescribe a reasonable retention period?

Reasonable retention periods will depend on the nature of the data and the purpose for which they are collected and the legal obligations and rights relating to the data. It would be difficult (if possible at all) to define a single retention period. While the goal is laudable, it is easier to state the principle that information should be maintained only as long as is necessary, than to attempt to implement such a specific requirement in a reasonable manner. For example, does "necessary" mean that payment transaction data need only be obtained until the purchased item is delivered, or may it be maintained for the statute of limitations during which either party may wish to sue or is subject to suit. If so, what is "necessary" for statutes of limitation that will be not be tolled until "discovery" of the breach giving rise to the suit (a period which can be decades for certain causes of action)? Is it "necessary" that analytics and aggregated anonymous information derived from the data be retained for the

longer but more indefinite periods during which retention may be "advisable" or "useful"? Further challenges to locking down a retention period arise when attempting to harmonize the multitude of data retention requirements which most companies are subject to (*e.g.* SEC reporting requirements, regulatory reporting requirements, and state Blue Sky law record retention requirements, etc.)

How should the substantive principles set forth in Section V(B)(1) of the report apply to companies with legacy data systems?

Providing (or insisting upon) consent to collection of data already collected, or to deal with commingled data, is probably impossible as a practical matter. However, at least as a theoretical matter legacy systems can be integrated into business processes which adhere to the principles of reasonable security, consistent and (as possible) retention periods. This is much easier said than done. Examples of some of the challenges will be: (1) managing use limitations where the legacy system cannot identify any privacy obligations which were generated at the time of collection; and (2) unwinding embedded use cases for data points which were not intended at the time of collection (*e.g.* using a publicly available identifying data point as an authenticator, with SSNs as a good example). In any event, the costs of retrofitting legacy systems (often requiring a complete redesign of a database structure) can be very significant.

D. <u>Commonly accepted practices</u>

Is the list of proposed "commonly accepted practices" set forth in Section V(C)(1) of the report too broad or too narrow?

The FTC's concept of "commonly accepted practices" appears to be an idea worth supporting: to the extent an appropriate list can be created, it would provide more certainty for all. The Report correctly notes that a person who presents a credit card should be deemed to know that it will be processed by service providers and payment system participants – what is important for data subjects to know is not that, but what *else* will be done with that data (if anything).

If a list of commonly accepted practices can be created, it would appear counterproductive to the objective of greater simplification to require companies to state the obvious in their privacy policies for the sake of transparency. By definition, a commonly accepted practice is inherently transparent. To ensure transparency, the FTC may wish to consider posting the list on its website: privacy policies could then include a URL for the list but otherwise be shortened to focus on *uncommon* uses of data or uses not otherwise on the list.

With respect to the Report's proposed list, we respectfully suggest that it is too narrow to be useful. A more useful starting point would be to build upon the lists in regulations implementing the federal Gramm Leach Bliley Act (see FTC's version at 16 C.F.R. § 313.13 through .15. Further, we respectfully suggest that the FTC continue to balance the community's interest in protecting itself within a category of secondary uses which are "commonly accepted practices" that do not require consent. By this, we mean anti-fraud and public protection services which maintain the integrity and trust in the commercial ecosystem. The financial and healthcare regulatory environments are good starting points for FTC review of this concept.

A question the FTC may wish to consider for the benefit of Congress, is whether, and to what extent, data aggregators fall within the definition of consumer reporting agencies and/or whether the FCRA should be amended to cover them. For example, databases of criminal convictions are built using public records and are available to any one willing to pay for a search; other data compilations are available for free. The terms of use for such sites typically preclude the user from using the information for a FCRA-covered or unlawful purpose and state that the website is not a consumer reporting agency. The question, in an Internet age, is whether FCRA applies, or should be amended to apply, to such sites? As noted, there are important public policy issues at stake. We note that legislation to achieve this result has been introduced in recent Congresses, but were not enacted into law. The issue illustrates, however, the need to adapt existing laws to new circumstances if warranted and as appropriate.

E. Special choice for online behavioral advertising: Do Not Track

The questions around universal choice mechanisms all have a similar set of challenges to be addressed. As discussed above, an underlying principle of any regulatory/enforcement framework will be the principle of context. Any "universal" choice mechanism will run into the problem of being non-contextual. As a consequence, choice mechanisms need not only to provide means to control the use of data in a behavioral advertising context, but also to provide appropriate notice of the parties involved as and when warranted. Considering that behavioral advertising can actually reduce the amount of advertising, there is direct benefit to the consumer when such activity is undertaken in a manner that stakeholders, including consumers, can view as responsible and transparent.

The online advertising ecosystem is complex and features a multitude of participants. As a consequence, any universal choice mechanism would need to be able to reach across all the participants in the ecosystem to be effective. This presents not only daunting technological problems, but also contractual problems. Unless the provider of a universal choice mechanism can be universally agreed upon by all participants in the advertising ecosystem, any choice provider brave enough to offer such a service may face significant potential liability.

Finally, most of the technological modes of tracking for behavioral advertising also have legitimate uses for other purposes. These other uses benefit the entire ecosystem. The website optimization, security, ID Management, and Search industries all use tracking to improve their services and, in some instances, directly protect consumers. Any attempt to regulate or legislate behavioral advertising, even through "soft" regulation, should remain technologically neutral and address only the activity determined to be objectionable – not the technology used to engage the activity. Failure to design a privacy framework that takes this into account might have unintended consequences that could well damage the continued development of e-commerce.