

# BITS

FINANCIAL SERVICES  
R O U N D T A B L E

July 14, 2009

Ms. Robin Layton  
Director  
Office of Technology and Electronic Commerce  
U.S. Department of Commerce  
1401 Constitution Avenue NW  
Washington, DC 20230  
via email: robin.layton@mail.doc.gov

Dear Ms. Layton:

BITS<sup>1</sup> appreciates the opportunity to participate in the Asia Pacific Economic Cooperation (APEC) Data Privacy Pathfinder pilot test. The following high-level comments and detailed appendices reflect both our commitment to providing meaningful feedback and our interest in the ultimate success of the program.

In addition to this written submission, BITS will be represented on the U.S. delegation to the APEC meetings in Singapore in July, and we would welcome any opportunity to discuss the APEC program with representatives of the Department or other stakeholders.

## **BITS' Pilot Participation**

BITS' original intention in the pilot was to combine the comprehensive applications of one or more member institutions with survey data compiled from throughout BITS' membership. BITS, however, was unable to garner completed applications to serve as the foundation for this process.

---

<sup>1</sup> The Financial Services Roundtable, of which BITS is a division, represents 100 of the largest integrated financial services companies providing banking, insurance, investment products and services to the American consumer. BITS leverages intellectual capital to address issues at the intersection of financial services, operations and technology. BITS focuses on strategic issues where industry cooperation serves the public good, such as security, fraud prevention, and critical infrastructure protection.

Member institutions with international operations that are also familiar with the proposed process and the draft Project 1 Questionnaire and Project 3 Assessment document found them to be problematic, and not tied closely enough to the APEC Principles, U.S. law, or the member economies in which they operate. These members invested substantial resources in preparing detailed comments, presented in this submission as Appendices A, B and C (described below). However, given their experience with the pilot documents, they were unable to draft completed applications for BITS to use in this exercise. BITS attaches significant weight to the experience of these institutions, not only because they are active enough to have well-developed perspectives on the APEC process, but also because they represent some of the largest, most international firms, with substantial stakes in Asia Pacific commerce.

As a result, rather than produce a single, representative, completed Questionnaire, BITS is submitting this letter, an Analysis of the Proposed Process (Appendix A), a Summary of Key Issues (Appendix B), and Comments on Questionnaire (Appendix C) received from our members. BITS gathered this input from our members' senior privacy, operations and technology executives. Given the diversity of BITS member institutions, the diverse roles of these executives, and the varying levels of engagement, it should not be assumed that all BITS members endorse all of the reported findings.

### **Program-Level Observations**

BITS' work in the pilot surfaced a couple of critical concerns inherent to the current Questionnaire/Assessment approach. First, even an extremely disciplined translation of the Principles into a checklist will, by definition, introduce new, detailed requirements. This introduction of new tests (whether they are extrapolations of Facing Page Commentary, culled from other compliance regimes, or developed de novo) unavoidably draws the discussion away from the original Principle and toward details that have less of a policy underpinning. Second, this translation also moves the discussion from the higher policy plane to the more formalistic execution of a checklist. While regulators in other arenas are migrating toward principles-based approaches, the Questionnaire/Assessment construct inevitably pulls this initiative toward a mechanistic, rules-based approach.

As currently contemplated, the APEC process is focused on assessments of the applicant companies, with little recognition of national or sectoral privacy regimes or the practical need for organizations to comply with the laws of economies in which they operate. We believe that this approach affords insufficient attention to the APEC commitment to be "respectful of requirements of individual economies." For example, in the U.S., policy choices have accumulated over time to form a national data protection approach, and the right to preserve that approach locally should be acknowledged in any APEC implementation, as it was in the APEC Framework. We urge the Department to work with the other economies to build enough flexibility into the system to allow for culture-specific interpretations of the Principles in those member economies. For example, the U.S. model presumes that data can be used for legitimate business purposes except where constrained by law, and the Principles should not be interpreted to reverse that presumption. An appreciation for existing norms will also eliminate layering of new

APEC requirements over existing local obligations. In the attached comments on the specifics of the Questionnaire, we identify a number of examples of this layering onto existing U.S. law.

The applicant-level approach also fails to capture the substantial efficiencies of recognizing that there are economies and industries in which existing legal requirements mandate practices that satisfy the APEC Principles. For example, under the current approach, individual financial institutions, whose practices already are subject to close scrutiny by state and federal examiners, would each have to demonstrate APEC compliance from a zero base. Capturing these efficiencies is absolutely critical in an environment in which prospective participants will carefully assess the costs and benefits of enrolling in the program.

BITS also has some concerns about the apparent conflation of the original objectives of the APEC Framework: (1) facilitation of cross-border data flows and (2) possible consideration by APEC economies that have no data protection laws. We believe that the Pathfinder and any further work on a subsequent program should be tightly focused on enabling frictionless data flows.

### **Document-Level Observations**

At the level of the documents themselves, BITS' attached comments on the Questionnaire and comments on specific questions in the Questionnaire should not be read as endorsing the Questionnaire/Assessment approach. These comments are provided in the spirit of setting aside our over-arching concerns and offering several focused observations. We look forward to future discussions with the Department of Commerce on the process.

Some questions, where the answers would be universal, need not be asked. For others, it should be clarified that representative responses, rather than exhaustive ones, would be sufficient. Institutions attempting to answer the questions as drafted and to substantiate those answers across geographies, customer segments, channels, and lines of business quickly found themselves mired in detail that ultimately was not useful in proving adherence to the Principle.

For certain Principles and certain questions, the Questionnaire specifies qualifications - often asking the applicant to cite those qualifications unless the response is an unconditional "yes." These recitations of the qualifications seem to imply that the citation is necessary to preserve the privilege, that the qualifications apply only to certain Questions and Principles, and that no other exceptions could be valid. Institutions, recognizing that few of their responses will be unequivocal and that there may be other culture-specific exceptions, found the named qualifications, on balance, to be more constrictive than helpful.

Comments on the Questionnaire, including examples of the questions apparently extending beyond the associated APEC Principle, are reflected in Appendix C, although these comments need to be read in conjunction with Appendix A and Appendix B.

## **Conclusion**

BITS appreciates the substantial effort that the Department and the various Pathfinder participants have devoted to drafting the associated documents and invested in conducting the pilot. As the process continues to move forward, we urge enhanced clarity of administrative and substantive expectations in order to realize the maximum net benefit to participating organizations and affected individuals.

We look forward to our ongoing collaboration with the Department on this initiative, and to contributing to the upcoming discussions in Singapore. Please feel free to phone me at 202 589-2440 or email me at [leigh@fsround.org](mailto:leigh@fsround.org) with any questions or other comments.

Sincerely,

A handwritten signature in black ink, appearing to read "Leigh Williams". The signature is fluid and cursive, with a long, sweeping underline that extends to the right.

Leigh Williams  
BITS President  
The Financial Services Roundtable

Attachments:

Appendix A – Analysis of the Proposed Process

Appendix B – Summary of Key Issues

Appendix C – Comments on Questionnaire

Copies:

Mr. Markus B. Heyder  
Federal Trade Commission  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
via email: [mheyder@ftc.gov](mailto:mheyder@ftc.gov)

Mr. Jeffrey M. Kopchik  
Senior Policy Analyst  
Technology Supervision Branch  
Federal Deposit Insurance Corporation  
550 17<sup>th</sup> Street NW  
Washington, DC 20429  
via email: [jkopchik@fdic.gov](mailto:jkopchik@fdic.gov)

## Appendix A – Analysis of the Proposed Process

**General Note:** The comments in Appendices A, B, and C are not answers to the Questionnaire, but illustrate some of the key issues identified to date. Comments on the Questionnaire in Appendix C do not reiterate all of the issues set forth in this Appendix A below. Therefore, the Analysis of the Proposed Process (Appendix A) and Summary of Key Issues (Appendix B), as well as the Comments on Questionnaire in Appendix C, must be read together so that key concepts and concerns are not overlooked. For example, the Comments on Questionnaire in Appendix C generally do not reiterate that the Questionnaire goes beyond the laws of other APEC economies. In addition, while U.S. law is broadly in compliance with the APEC Principles, the Appendix C identifies many places where the Questionnaire goes beyond U.S. law as well as beyond the APEC Framework. Appendix C, however, does not attempt to exhaustively list all such places.

The APEC Framework recognizes that “[a]s both business operations and consumer expectations continue to shift due to changes in technology and the nature of information flows, businesses... require simultaneous input and access to data 24-hours a day...” In other words, in the world of global data flows and multinational organizations, data no longer flows in a point-to-point manner but in a global networked environment. Thus, in order for businesses to meet customer needs and provide efficient services, governments must refrain from unduly restricting the global flow of data. The APEC Framework expressly acknowledges this objective when it states that “the free flow of information [is] essential for both developed and developing market economies to sustain economic and social growth” and “[r]egulatory systems that unnecessarily restrict this flow or place burdens on it have adverse implications for global business and economies.”

In order to achieve this objective, the APEC Framework further recognizes that nations may make different choices regarding the protection of certain information even when they agree on the broad principles that apply. Moreover, the choices that governments make are not just in the obligations they impose— the exceptions from those obligations also reflect each government’s policy choices. For example, based on the sensitivity of the data, the U.S. has chosen to provide more protection for customers of financial institutions and health care providers than for other types of customers and data. It also allows organizations to provide information to the government for a variety of purposes. None of these carefully constructed solutions should be rejected lightly and the APEC Framework recognizes that these choices should be honored, rather than overridden. The Framework simply requires that local law be “broadly compliant” with the APEC Principles. As the Framework states, “[it] is not intended to impede governmental activities authorized by law when taken to protect national security, public safety, national sovereignty or other public policy” and “[i]n view of the differences in social, cultural, economic and legal backgrounds of each member economy, there should be flexibility in implementing these Principles.”

Allowing governments flexibility to implement the Principles in a manner consistent with their national circumstances is also the only way to avoid layering significant new

regulatory burdens on top of local laws addressing the same issues. The APEC Framework was designed to be a model for countries that do not have privacy laws and to facilitate cross border data transfers by eliminating unnecessary restrictions. The Questionnaire appears to have combined these two purposes and instead of facilitating cross border transfers, it creates a new free-standing, detailed and prescriptive data privacy regime. This new comprehensive international data privacy regime would apply to all participating organizations, in all APEC economies, in all situations. Such an approach deviates from the original intent of the APEC cross border initiative in a manner that would impose heavy new burdens that go beyond requirements currently imposed on organizations in the U.S. and other APEC member economies, and therefore imposes unnecessary burdens on global commerce in general.

Some EU member states have increasingly recognized that a prescriptive, rules-based approach to data privacy is problematic. A recent report published by the UK's Information Commissioner's Office concludes that the EU must move away from its current model, which focuses on compliance with formalities, and move toward a model that focuses on fundamental principles.<sup>2</sup> Contrary to this more flexible approach being considered elsewhere, the Questionnaire has moved toward a formalistic and prescriptive approach that will unnecessarily burden rather than promote the free transfer of data.

Set out below are some of the significant issues, including some that go to the issue of practicability, which are raised by the current approach as embodied in the Questionnaire and Assessment document. The role for individual organizations should be to represent that they have policies, procedures or codes directing them to follow local law with regard to personal information.

## **I. Discussion of the Issues**

### ***1. The Questionnaire requires each participating organization to comply with a new, detailed, free-standing and prescriptive legal regime that does not reflect the social, cultural, economic and legal backgrounds of each member economy in which it operates.***

These documents create a certification scheme in which each participating organization is required to obtain certification that its privacy practices meet new data collection, use, and disclosure rules. When the Assessment document and the Questionnaire are read together, it is clear that if a company does not answer "yes" to each question or cite an applicable qualification that it is not in compliance with the relevant Principle. For virtually every question, the Assessment document indicates that where an applicant answers "no" and does not identify an applicable qualification, the accountability agent must inform the applicant that it is not in compliance with the Principle. Since each company rather than each economy currently is expected to fill out the Questionnaire, such an approach turns the Questionnaire into a rigid standard to be applied to all

---

<sup>2</sup> NEIL ROBINSON ET AL., RAND EUROPE, REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE (2009).

participating companies regardless of the economic, legal, and social contexts in which they operate.

This approach combines the objective of encouraging governments to refrain from undue restriction of cross border restrictions with the use of the APEC Principles more generally. In any case, the current approach places the burden on organizations and bypasses the flexibility needed at the economy level that is anticipated by the Framework. For example, particular determinations made at the national level concerning when and where to provide customers notice/choice and access to data would be obviated. As a consequence, broad-based national determinations about how to implement the Principles, including those made by countries such as the U.S., which has considered its national circumstances and as an economy is already in compliance with the APEC Principles, would not be recognized.

***2. Participating organizations are required to comply with the new comprehensive APEC regime in addition to local law.***

It would be troubling enough if companies only had to worry about compliance with a new standard that has not been tailored to their national circumstances. However, as the Framework states, “organizations [will] still be responsible for complying with the local data protection requirements as well as local law.” Thus, participating organizations would have to comply with a new comprehensive, detailed, prescriptive and overlapping data privacy regime, as reflected in the Questionnaire, in addition to local laws. As discussed above, this was not the intent of the Framework.

***3. The Questionnaire adds new requirements that are not contained in the Framework, that go beyond the law of the U.S and other APEC member economies.***

The approach need not require that each of the APEC Principles is reestablished. However, the Questionnaire takes the Principles and goes far beyond even that, adding new requirements to them, limiting the flexibility to collect, use and disclose data currently available to applicants under local law, removing all of the flexibility from the process and requiring organizations to expend enormous efforts describing how they comply with the new requirements. The new requirements go beyond the APEC Principles themselves, the law of the U.S., and other APEC member economies. For example, question 5 requires companies to notify individuals that their personal information may be subject to an international transfer. This goes beyond what is required by the Framework. It also goes beyond U.S. law and, most likely, the law of many other APEC member economies. Similarly, the requirement contained in several questions in the Notice section to provide copies of all applicable notices goes beyond requirements in the U.S. and the EU BCR process. Such granular requirements place the burden on individual companies to prove that they meet a rigid regional standard that is likely inconsistent with their domestic economic, legal and/or social circumstances.

The approach taken by the Questionnaire is more similar to that of the EU, where data cannot be collected, used or disclosed unless you have a legal basis. For example, in the

Collection and Use section of the Questionnaire, it appears that the collection and use of data has to be pursuant to an identified, relevant or compatible/related purpose unless it is used as “expressly authorized” by law or by consent. Such an approach is fundamentally inconsistent with the manner in which most APEC economies deal with data protection. In most APEC economies, including the U.S., there is a presumption that data can be collected, used and disclosed unless there is a specific prohibition.

***4. The Questionnaire asks companies to provide information concerning their policies and practices in a volume and level of detail that is wholly impracticable.***

In order to accurately and completely answer the questions requiring a description of all relevant circumstances, a multinational company engaged in complex, global data flows in multiple business lines would have to expend significant time and resources, and answering the question would still not be practicable. This problem arises in many parts of the Questionnaire, particularly where it requires applicants to provide copies of all of applicable notices and repeatedly asks applicants to describe all the means it employs to fulfill a particular requirement. For example, question 18 asks an applicant to describe all the ways in which its collection practices are lawful, fair and consistent with the jurisdiction that governs collection. It would not be practicable for an organization to provide such an exhaustive description, nor would it be practicable for a member economy to describe all the ways in which its laws impose such requirements.

***5. Qualifications***

***a) The qualifications are not assumed to apply or expressly deemed to be outside the scope of what is covered and they must be raised and established by each organization.***

As it stands now, the Questionnaire essentially presumes that no qualifications apply to an organization unless it specifically raises them and describes their application in all circumstances. Again, in order to accurately and completely document all the situations in which a qualification may apply, a multinational company engaged in complex, global data flows in multiple business lines would have to expend significant time and resources. Such a burden is inconsistent with the Framework’s recognition that “the free flow of information [is] essential...to sustain economic and social growth.” This burden would be eliminated if the Questionnaire made it clear that all relevant qualifications are assumed to apply or if it were otherwise established that such situations are outside the scope of what is covered.

In addition to being extremely burdensome, this approach could have other harmful consequences. If a participating organization fails to assert all of the relevant qualifications or misapplies the qualifications, that organization could lose the ability under the APEC regime to move data across border in certain situations despite the fact that it has the right to do so today under local law. For example, the Gramm-Leach-Bliley Act contains numerous reasonable and appropriate exceptions, such as the exception for disclosures to law enforcement. If an organization in the U.S. failed to detail all the situations in which such an exception could apply, moving data pursuant to

that exception in such situations would not be permitted under the current approach. This would not only have adverse consequences for the organization but would undercut the legitimate interests of the government that established the exception.

Finally, this approach is simply not appropriate when applied to certain member economies. As stated above, the approach taken by the Questionnaire is fundamentally inconsistent with the manner in which most APEC economies deal with data protection. It does not make sense to require organizations operating under such a system where collection, use and transfer of data is generally permitted unless expressly prohibited by law to cite to and reestablish specific qualifications that permit them to collect, use and transfer data in the way that they do.

**b) *The qualifications do not apply to all relevant Principles.***

The Questionnaire inaccurately suggests that qualifications only apply to a few Principles rather than applying broadly wherever they are relevant. For example, the qualification regarding action in emergency situations only appears in the Notice and Choice sections. This implies that companies are not relieved of any of their responsibilities under the other Principles in the event of an emergency. It must be made clear that the qualifications apply to all relevant Principles or are otherwise outside of the scope of what is covered.

**c) *The qualifications are overly narrow.***

The commentary to article 13 allows great flexibility and permits additional breadth to exceptions: “Economies implementing the Framework at a domestic level may adopt suitable exceptions that suit their particular domestic circumstances.”

The Questionnaire deviates from this approach in two ways. First, it purports to provide a comprehensive list of qualifications that fails to include many exceptions a member economy might choose to apply. For example, the Gramm-Leach-Bliley Act contains exceptions for actions required for institutional risk control; the provision of information to attorneys, accountants and auditors; the provision of information to government institutions or self-regulatory groups; actions to comply with Federal, State or local laws; and actions to prevent actual or potential fraud. The qualifications contained in the Questionnaire, however, would not cover some of these situations.

Second, the qualifications that are contained in the Questionnaire are defined too narrowly. For example, a qualification contained in the Questionnaire permits disclosure to a government institution only when the government has issued a warrant or a subpoena. In the U.S., however, there are other lawful forms of process by which the government can seek the disclosure of information, and in certain other countries, the form of process is likely to be even more diverse. Furthermore, this regime appears to exclude other appropriate disclosures, such as those in connection with litigation, potential litigation or other legal claims, or when governments make informal requests for information, or when it provides incentives, such as reduced penalties, for voluntary

disclosure of possible violations (e.g., with regard to the Foreign Corrupt Practices Act), or simply when companies voluntarily provide the government with information concerning potential criminal activity in an effort to be a good corporate citizen.

New qualifications should be added and existing qualifications broadened or it should be made clear that they are outside of the scope of what is covered, so that they encompass any reasonable qualification a member economy might choose to establish.

## Appendix B – Summary of Key Issues

Below is a summary of some of the key issues that have been identified to date and are discussed further above. These issues need to be addressed and should guide the future direction of any further work:

- Any approach must recognize, just as the APEC Framework recognizes, that data no longer flows in a point-to-point manner but in a global networked environment. Thus, in order for businesses to meet customer needs and provide efficient services, governments must refrain from unduly restricting the global flow of data.
- The Questionnaire and Assessment documents do not maintain a focus on ongoing responsibility for the transfer of data between countries where appropriate, such as in the case of service providers. They are not currently focused on the original objectives, but instead have combined them and propose a new comprehensive international data privacy regime that imposes heavy new burdens on participating organizations and unnecessary burdens on global commerce in general.
- Instead, they create a certification scheme in which each participating organization is required to follow a complicated process to obtain certification that its privacy practices meet new data collection, use, and disclosure rules that go beyond U.S. law, the laws of other APEC economies and even the APEC Principles themselves.
- The two objectives of the APEC Framework should not be combined; the approach should be streamlined to focus on responsibility for cross border transfers where appropriate, such as in the case of service providers.
- The approach should not require that each of the APEC Principles is reestablished, but in any event, it should not create new requirements that go beyond the APEC Principles.
- It is not appropriate or workable to require organizations to hew to a standard that was not designed to be applied in minute detail and which goes beyond the laws of the countries in which they operate and does not reflect the national circumstances of those economies.
- Organizations have to comply with local data protection laws where they operate. They should not have to demonstrate compliance with another comprehensive data privacy regime where the requirements are inconsistent with those in the countries in which they operate.
- Broad-based national determinations about how to implement the Principles, including those made by countries such as the U.S., which has considered its national circumstances and as an economy is already in compliance with the APEC Principles, must be recognized. For example, particular determinations made by member economies

concerning when and where to provide to customers notice/choice and access to data would be superseded.

- The approach also needs to be consistent with that of the U.S. and other APEC member economies. Currently, the APEC pilot is following a path where data cannot be collected, used or disclosed unless there is a legal basis. The current detailed prescriptive documents, which individual participating organizations must adopt, are fundamentally inconsistent with the manner in which most APEC economies, including the U.S., deal with data protection, where there is a presumption that data can be collected, used and disclosed unless there is a specific prohibition.
- The approach needs to reflect the flexibility that was built into the APEC Framework, which expressly states that “[it] is not intended to impede governmental activities authorized by law when taken to protect national security, public safety, national sovereignty or other public policy” and “[i]n view of the differences in social, cultural, economic and legal backgrounds of each member economy, there should be flexibility in implementing these Principles.”
- “Qualifications” (exceptions to the Principles) must be assumed to apply so that they do not have to be specifically raised and established for each relevant question. Alternatively such situations must be deemed outside the scope of the APEC project. In addition, it should be made clear that these “qualifications” are applicable to all relevant Principles or are otherwise deemed outside the scope of the APEC project. Moreover, new qualifications should be added, and existing qualifications should be broadened, both in their scope and their application, so that they encompass the approach taken by APEC economies and the reasonable exceptions that a government might choose to apply. Such circumstances include, for example, actions for required institutional risk control or compliance; the provision of information to attorneys, accountants and auditors; provision of information to government institutions or self-regulatory groups; actions to prevent actual or potential fraud; and actions in connection with litigation, potential litigation or other legal claims.
- The approach also needs to be more general and practical. The APEC proposal requires that certification itself be obtained through completion of the complex Questionnaire, requiring companies to provide information concerning their policies and practices in a volume and level of a detail that is wholly impractical for a multinational company engaged in global data flows in multiple business lines. Just as it would be impracticable for a member economy to describe all the situations in which its laws impose the relevant requirements, it would be impracticable for an organization to provide such an exhaustive description.

## Appendix C – Comments on Questionnaire

### I. General Comments

The questionnaire essentially presumes that no qualifications apply unless they are specifically raised and their application is described for all circumstances. It would be difficult for organizations to identify, raise and describe the application of all relevant qualifications, particularly if an organization does not regularly invoke qualifications because it operates in a system where there is a presumption that data can be collected, used and disclosed unless there is a specific prohibition. If an organization failed to assert all of the relevant qualifications, the participating organization could lose the ability under the APEC regime to move data across borders in certain situations despite the fact that it has the right to do so under local law.

Qualifications cannot be limited to the narrow list of qualifications contained in the questionnaire. This approach is consistent with the APEC Framework, which states, “Economies implementing the Framework at a domestic level may adopt suitable exceptions that suit their particular domestic circumstances.” The qualifications, as written, fail to capture the approach or qualifications member economies have established in their domestic laws. In addition, the questionnaire indicates that qualifications only apply to certain principles. For example, there are no qualifications listed in the Accountability section.

The qualifications, at a minimum, should address the following:

- i. **Disclosure to a governmental institution or self-regulatory group:** Disclosures of personal information to law enforcement agencies, other governmental institutions, or non-governmental self-regulatory groups.
- ii. **Actions taken to prevent actual or potential fraud**
- iii. **Actions taken for the purposes of risk control or compliance:** Including disclosures made to parties such as accountants, lawyers, and auditors.
- iv. **For legitimate investigation purposes:** Investigations of a violation of a code of conduct, a breach of contract or a contravention of the law where an organization operates.
- v. **Actions in connection with legal claims:** Actions in connection with litigation, pending litigation or other types of legal claims.
- vi. **Actions in the event of an emergency:** Emergency situations that threaten the life, health or security of an individual.

- vii. **Publicly-available information:** Where the Personal Information controller is collecting, using or transferring publicly-available information.
- viii. **Protection of confidential information:** Where confidential or privileged information would be exposed.
- ix. **Protection of information of others:** Where the information privacy of others would be violated.
- x. **Third-party receipt:** Where personal information is received from a third-party.
- xi. **Where collection, use or disclosure is obvious:** Where the collection, use and/or disclosure of an individual's personal information would be obvious to a reasonable individual, including use of business contact and other professional information.
- xii. **Impracticability:** Where actions would be impracticable.
- xiii. **Disproportionate burden:** Where the burden or expense would be unreasonable or disproportionate to the risks to the individual's privacy.
- xiv. **Consent:** Where an individual has given implied or explicit consent for personal information to be collected, used and/or disclosed in a particular manner.
- xv. **Necessary to provide a service or product:** Where the Personal Information controller would be impeded in providing a service or product requested by that individual.

The qualifications must be broadened, they must be assumed to apply, and it must be clear that the qualifications are applicable to all relevant principles.

## II. Specific Comments

### Notice

Generally:

This section goes beyond U.S. law to the extent it requires organizations to give notice that are not currently required to do so by local law.

Questions:

1. The questionnaire asks for copies of the applicable notices throughout this section. It would be impracticable for a large multinational company engaged in complex, global data flows in multiple business lines to provide a copy of every notice.

3. GLBA requires companies to provide examples of information collected rather than to identify all of the purposes.

4. It is not clear what “third parties” means. It should be made clear that it does not include affiliates. Otherwise, notice requirements as well as requirements found throughout the questionnaire would apply to intra-company transfers, making this approach completely impracticable.

5. This question goes beyond what is required by the APEC Framework; it also goes beyond what is required by U.S. law.

8. This question goes beyond U.S. law.

10. This question goes beyond what is required by the APEC Framework.

Qualifications:

ii. This qualification needs to be broadened to encompass all forms of impracticability. The APEC Framework speaks broadly of impracticability and provides technological impracticability as an example.

iv. This qualification needs to be broadened. There are situations where it is reasonable for an organization to disclose personal information to the government. There are methods by which governments can require organizations to provide them with information that do not involve warrants or subpoenas. The APEC Framework states that the principles should not impede such efforts by governments. Furthermore, there are situations in which an organization would voluntarily disclose information to the government. In some cases, the law offers incentives, such as reduced penalties, for voluntary disclosure of information. In other instances, an organization may provide a government with information about potential criminal activity simply because it wants to be a good corporate citizen. This qualification needs to be expanded to encompass all these situations.

### Collection Limitation

Introductory Language:

This entire section goes beyond U.S. law. When notice is required, U.S. law generally requires organizations to give consumers examples of the types of data collected and the types of entities to which data might be disclosed.

The APEC Framework does not talk about “stated purposes”. This language suggests that data can only be collected for a purpose that was mentioned in a notice. For a large multinational company, it is impracticable to come up with a comprehensive list of all the purposes for which the data is collected.

Questions:

12, 17, 19. These questions go beyond what is required by the APEC Framework.

18. It is not clear what the phrase “lawful and fair means” refers to. The APEC Framework suggests the term “unfair means” refers to those means that, although not expressly prohibited by statute or regulation, are not permitted in the relevant jurisdiction. It must be clear that this phrase is not imposing a new “fairness” standard. Also it would be impracticable for an organization to describe all the ways in which it collects data by lawful and fair means.

### Uses of Personal Information

Generally:

This section goes beyond U.S. law. U.S. law generally permits the use of personal information and only limits its use in certain identified situations, such as financial information shared with unaffiliated third parties.

Questions:

20-25. These questions go beyond what is required by the APEC Framework

### Choice

Generally:

This section goes beyond U.S. law in many respects. For example, in certain circumstances, under U.S. law, consumers are given the choice to opt out of disclosures to certain unaffiliated third parties.

Questions:

26, 27. It would be impracticable to describe all mechanisms for individuals to exercise choice. Moreover, under U.S. law, individuals may exercise choice by choosing not to do business with an organization.

32. This question goes beyond what is required by the APEC Framework.

### Integrity of Personal Information

Generally:

This section goes beyond U.S. law in many respects. U.S. law requires mechanisms for correction in certain situations, such as in the credit reporting context where an error will clearly have a material impact on the individual.

Questions:

34. It would be impracticable for an organization to describe all mechanisms for correcting inaccurate, incomplete and out-dated personal information.

35-37. These questions go beyond what is required by the APEC Framework and beyond what is required by U.S. law.

### Security Safeguards

Generally:

This section goes beyond U.S. law in many respects. Under U.S. law, organizations are required to make sure that they assess and manage reasonable foreseeable risks and that their service providers have adequate security safeguards.

Questions:

39, 40, 45. It would be impracticable for an organization to describe all safeguards implemented to protect personal information and to describe all the risks of harm and how each safeguard is proportional to that risk.

41-47. These questions go beyond what is required by the APEC Framework.

### Access and Correction

Generally:

This section goes beyond U.S. law in many respects. Under U.S. law, access and correction is provided in certain circumstances, such as credit eligibility where the decision would have a material impact on individuals.

Questions:

48. It would be impracticable for an organization to describe all situations where an organization provides confirmation of whether or not it holds personal information about the requesting individual.

49. This question goes beyond the language of the APEC Framework and it would be impracticable to describe all such policies/procedures.

50. It would be impracticable for an organization to describe all situations where an organization permits requesting individuals to challenge the accuracy of information and to have it rectified, completed, amended or deleted.

### Accountability

Generally:

This section goes beyond U.S. law in many respects. U.S. law requires companies to assess, manage and control reasonably foreseeable risks and to use service providers with adequate security safeguards.

Questions:

51-64. These questions go beyond what is required by the APEC Framework.

51, 60, 61. These questions mix mechanisms that would be applicable to service providers with mechanisms that would be applicable to affiliates.

53. In a global organization, different functions will be responsible for different aspects of information privacy.

58. This question is very granular; other regulatory regimes do not require this level of detail.

59. It is not clear what the distinctions are among personal information processor, agent, contractor and service provider.