Public Safety and Domestic Security Considerations in Drafting and Implementing the Privacy Framework

The United States Department of Justice (hereafter "USDOJ" or "Department") is pleased to be part of the Domestic Implementation Workshop: a workshop designed to assist economies in reviewing, amending, drafting and/or passing privacy laws in order to give effect to the APEC Privacy Framework (Framework). Bearing in mind that the Framework is the product of extensive efforts by a number of APEC economies, and recognizing the significance of privacy in promoting business and enabling cross-border data flows, the Department would like to provide the following drafting tips, relating to public safety and domestic security, for economies to consider when implementing the Framework.[1]

This summary has been designed by the Department in order to provide what we hope is valuable insight into how law enforcement and domestic security agencies can work with privacy directorates/agencies to implement a comprehensive privacy strategy that enhances privacy throughout the region while enabling the continued enforcement of an economy's criminal laws, protection of an economy's citizens, and investigation/apprehension of those criminals who would violate an economy's laws, such as stealing the personal information of another.

The following drafting tips are provided in the order that they appear in the Framework so that they will be easier to consult as economies begin to implement the Framework.

I. Framework - Scope Section

Pursuant to the Scope Section of the Framework (Part II), economies are permitted to take exceptions to the Privacy Principles if they are "limited and proportional to meeting the objectives to which the exceptions relate; and, [are] made known to the public; or, [are] in accordance with law."

One key question that could arise in implementing this exception provision is whether the exception is meant to be applied as a general rule, to a whole category of activity or information, or whether the exception is meant to be applied on a case-by-case basis. So what does it mean to apply the exception to a category of information or on a case-by-case basis? Perhaps an example will help illustrate this concept.

For purposes of our example, let's assume that a legislature decides to enact a law that allows businesses to voluntarily provide to law enforcement any information that they may acquire pertaining to a crime, which has not yet been committed, but will be committed in the future. Let's also assume that a company, Company A, while servicing a computer server, finds an E-mail that relates to a bombing of a building that is supposed to occur the very next day. Obviously, this information is quite sensitive and

[1] Please note that this white paper summarizes the views of the U.S. Department of Justice and does not necessarily represent the views of the entire U.S. Government.

timely, as well as very necessary to aid both intelligence and law enforcement agencies in preventing the attack.

If we were to apply the exception under the Framework to a whole category of information, -- say a law that allows businesses to provide information to law enforcement that relates to a future crime -- the company would not have to perform any additional review of the privacy implications of providing this information to the law enforcement agency. Furthermore, they would not have to ask for some sort of exception to the Framework for this specific case - actions which could cost valuable time and possibly lives, and which could potentially alert the terrorists to the fact that the authorities have been informed.

By contrast, if a law were to apply the exception on a case-by-case basis, it might, for example, require the company or an outside party such as a judge or government privacy officer, to weigh the need for disclosure in this case specifically. This alternative might require the company to engage its own internal privacy review of the implications of supplying this information to law enforcement, seek an exception to its normal privacy policy for this specific case, and notify or seek approval from the designated privacy authority, prior to its disclosure. Each of these steps, in itself, could be a time consuming process - and, taken together, would likely result in the company not providing information to the authorities in time to stop the bomb and save lives.

In essence, if exceptions are applied on a case-by-case basis, the ability to prevent, investigate and fight crime and terrorism would be substantially hindered, if not rendered impossible. If a law were to require that exceptions be taken in each individual case, as opposed to one time, on a category of information or activity, decisions could not be rendered within the expedient timelines often needed to prevent crime and terrorism - whether it is a bombing of a building, or the theft of an individual's personal information from a credit card company's database server. Moreover, by permitting decisions on a case-by-case basis, a law runs the very real risk of inconsistent results in similar fact scenarios (depending upon the judgment, expertise and knowledge of the individual performing that analysis).

As such, the more workable solution is for economies to take exceptions to the Framework on categories of information or activities. This way, legislatures can enact public safety and domestic security laws that protect everyone, and handle the privacy implications of such laws at the time of enactment.

II. Framework - APEC Privacy Principles

Principle 1. Preventing Harm

In drafting privacy laws that give effect to Principle number 1, it is important to bear in mind that not all privacy infringements are bad. Some infringements actually protect privacy rights.

The reality of the matter is that when a law enforcement entity executes a search authority to search a home, or utilizes a court order to intercept the content of a communication, it does in fact infringe privacy. But is this infringement unlawful? The answer is no. Is this infringement necessary? Yes - if one hopes to apprehend the criminal and stop the crime. At the same time, it is important to bear in mind that these types of "lawful" infringements actually enhance and aid privacy.

For example, a lawful infringement of privacy by a law enforcement official may be necessary when that official is investigating a criminal who has been misusing the personal information of others by stealing their identities. In this example, let's assume that in order to commit this crime, the criminal has been gaining unauthorized access to a company's credit card database and stealing account holder names, credit card numbers, and other personal information. In such a crime, the primary evidence that exists to track the criminal might be the access and identification logs identified by the company as suspicious, as well as the account information of those customers whose information was accessed by the criminal without authorization.

In this situation, disclosure to law enforcement officials of the log records and customer records enhances privacy, because disclosure permits law enforcement officials to investigate the crime, interview victims, recover the stolen personal information, and prevent the data from being further disseminated. Additionally, by successfully bringing the criminal to justice, disclosure of the information could deter other would-be criminals from making the attempt to steal similar personal information, since it would be clear to those criminals that they will be investigated, arrested, prosecuted, and punished for those crimes.

When crafting laws that prohibit or punish privacy infringements, we should therefore qualify the references in those laws to make sure that they only cover "unlawful" privacy infringements. To further ensure that such laws are not misapplied to legitimate public safety or domestic security activities, our privacy laws could also define "unlawful" privacy infringements as excluding those actions that infringe privacy but are taken pursuant to a domestic statute, or are authorized by a court of law or properly issued legal process. In sum: privacy statutes should focus on "unlawful" privacy infringements, not all privacy infringements.

Principle 2. Notice

With regard to the drafting of privacy laws that require the provision of notice to

individuals, it is worthwhile to consider how the requirement of notice under the Framework could potentially impact law enforcement. Specifically, a requirement that investigative governmental organizations notify subjects of investigations each time they undertake an investigation would be disastrous for public safety and domestic security. Once again, an example might be helpful to illustrate.

For example, if a law enforcement agency were investigating a kidnapping, some of the evidence that agency might wish to gather could include tracing the origin of phone calls made to the victim's family by the kidnapper-- or securing disclosure of the contents of the E-mail account used by the kidnapper-- all in the hope of finding some way to identify the location of the kidnapper. In order to collect this information, the law enforcement agency might use legal process to compel a phone or internet provider to provide information about the phone used to make the ransom demand calls, the times, dates and locations that the kidnapper logged in to the E-mail account, etc. Under such circumstances, if law enforcement were required to notify the customer (here: the kidnapper) that it is collecting his personal information, he would undoubtedly change his location to avoid capture. Worse, such notification could result in harm to the victim.

In short, the collection of personal information by law enforcement and domestic security agencies, pursuant to lawfully authorized process, is always a distinct possibility in any economy. The provision of notice of these collection processes would harm the underlying investigation, as well as pose additional threats to public safety. Under such circumstances, it would therefore be advisable that any privacy law or rule implemented requiring notice of collection contain an explicit exception to the notice requirement for personal information collected by law enforcement and domestic security agencies, pursuant to lawfully authorized process.

Conversely, the law or rule could require that every information controller that collects personal information provide a disclosure to individuals that their personal information may be collected and disclosed to law enforcement and/or domestic security agencies pursuant to lawfully authorized process, without any type of notice being provided to individuals at the time of the collection or disclosure.

For example, in the U.S., a notice used by some medical offices reads as follows:

We will disclose your health information when we are required to do so by federal, state and other law… We will disclose your health information when ordered in a legal or administrative proceeding, such as a subpoena, discovery request, warrant, summons, or other lawful process. We may disclose health information to a law enforcement official to identify or locate suspects, fugitives, witnesses, victims of crime or missing persons.

Principle 3. Collection Limitation

Principle number 3 notes that "[t]he collection of personal information should be limited to information that is relevant to the purposes of collection and any such

information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned."

In order to conduct law enforcement investigations, prevent terrorism, and fight crime, law enforcement will sometimes use legally authorized, non-public investigative means, such as: search authorizations, real-time interception of content (of voice or electronic communications), accessing of stored electronic communications (such as E-mail), etc. In assessing the privacy implications of these investigative mechanisms, it is important to bear in mind that each of these mechanisms is usually authorized by a domestic law requiring court intervention and review. Moreover, each of these mechanisms often has it's own privacy protections built in.

For example, in the U.S., access by law enforcement to the stored content of unopened electronic messages requires the issuance of a search warrant by a judge. In order to secure this search warrant, the law enforcement officer must first draft a number of documents, which provide information justifying the search, identifies the specific accounts to be searched (to avoid over-breadth), etc. Once the search warrant is drafted and submitted to the court, the judge then reviews the documents and determines whether or not the law enforcement officer has met his burden of proof. It is worthwhile to note that the burden of proof for securing a search warrant is one of the highest of any investigative tool. Even after the search warrant is approved, there are additional privacy protections implicated by the search warrant. For example, in traditional search warrants, if the search exceeds the scope of the warrant, there is a possibility that evidence seized during that search could be suppressed by the court.

Although search procedures vary considerably between economies, what hopefully becomes clear from the foregoing analysis of U.S. search warrants is that economies often have numerous privacy protections already built into different stages of the use of an investigative mechanism. These privacy protections were built in by the legislatures that created them -- at the time the mechanisms were created -- balancing the need to preserve privacy with the needs of the investigation itself, and the desire to preserve public safety.

Thus, one concept that laws generally do not require -- during initial implementation of these mechanisms -- is prior notice of their use, or expeditious disclosure of the information captured, as either of those would compromise the integrity of the investigation, tip off the criminal, and potentially result in harm to others. It is worth noting, however, that in the U.S., most of these tools do require notice after the investigation is completed. [2]

In drafting privacy laws, we should therefore be careful to exempt information

[2] In the U.S., to the extent that laws authorizing investigative tools do require notice to the subject individual at the time of use of the investigative tool, these laws usually include provisions for delaying notice until after the investigation, if deemed necessary.

collection by governmental, law enforcement and domestic security agencies from any privacy laws that create general collection limitations. As discussed in the notice section above, we should also be careful to exempt governmental, law enforcement and domestic security agencies from any privacy laws that requires prior, concurrent, or expedient notice, after the fact, of the collection of personal information, to the extent the collection is authorized by law or legal process.

Principle 4. Uses of Personal Information

Principle number 4 states that "[p]ersonal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect."

Due to the fact that private industry owns, operates and manages a large part of our economies' infrastructures, they are often the first to see evidence of crimes. For example, when a criminal engages in the theft of credit cards or unauthorized banking transactions, the card issuer or bank will presumably receive complaints from victims, or notice unusual patterns, at an earlier stage of the criminal process than will law enforcement officials. Moreover, as more and more industries move their operations online, they may also learn of criminal activities through criminal misuse of their own systems. Similarly, E-mail and web hosts might stumble upon evidence of a crime while engaging in routine maintenance of their systems - for example, discovering E-mails relating to a plan to molest a child.

As a result of industries' unique vantage point, an essential part of fighting crime is the voluntary cooperation that they provide to law enforcement officials. When looking at the issue of voluntary cooperation, however, it is important to take note of the fact that voluntary cooperation from private industry in fighting crime is already difficult to secure. For example, the 2004 annual Computer Crime and Security Survey, conducted as a joint initiative by the FBI and the Computer Security Institute, illustrated that only 20% of those U.S. companies suffering serious cyber-attacks on their systems in the previous year had actually reported those attacks to law enforcement (down from 30% in 2003). Indeed, in the U.S., we have spent a great deal of time encouraging the creation of public-private information sharing mechanisms, such as the FBI's Infraguard program or the Secret Service's Electronic Crimes Task Force. Nonetheless, some of the concerns raised by companies include bad publicity, angering the hackers and thereby bringing on additional attacks, losing customers, etc.

The last thing we want to do is create additional disincentives to voluntary cooperation through the implementation of privacy laws that do not explicitly allow for this type of cooperation. For example, wouldn't we want to permit the E-

mail provider that stumbled upon the E-mails relating to child molestation to report that to the police, and hopefully stop the actor before he is able to molest the child? Yet if a privacy law allowed the use of such information only to fulfill the purpose of collection or a related purpose, such a privacy law could actually hinder voluntary cooperation because neither of those reasons would be applicable when a provider inadvertently stumbles upon evidence of crime.

Similarly, none of the exceptions contained in Principle 4 would permit such voluntary sharing. Specifically, exception (a) would not apply since the company would not want to seek the consent of the individual whose personal information was collected since that would tip off the criminal and risk harm to the child. Exception (b) would not apply because the information is not being disclosed in order to provide a service or product required by the individual. And exception (c) would not apply because we are discussing "voluntary" sharing of information with law enforcement officials - not mandatory sharing "by the authority of law and other legal instruments, proclamations [or] pronouncements of legal effect."

In order to equip public safety organizations to fully protect their citizens, economies must encourage reporting, and not create additional burdens or disincentives that might discourage businesses from doing so. As such, privacy laws that restrict the use of personal information should be drafted to take into account the need for private industry to be able to voluntarily share information with law enforcement and domestic security agencies when it relates to a crime or a threat to domestic security. The Privacy Framework takes into account this need in the Scope Section by allowing laws to have exceptions for law enforcement, domestic security, and public safety reasons.

Principle 5. Choice

In considering legislation implementing Principle 5, it is important to bear in mind that while providing choice to individuals is undoubtedly an important privacy protection, there are situations when providing choice would not be appropriate.

For instance, very few, if any, criminals would voluntarily choose to have their personal information shared with law enforcement investigators. As such, for a law to require that a criminal target be given a choice as to whether his personal information may be shared with law enforcement agencies before the data is transferred would be an invitation to abuse and would surely result in harm to the public. Indeed, given a choice, a criminal or terrorist would likely choose not only to prevent his information from being shared, but would also choose to not have his personal information collected in the first place, so as to limit his evidentiary trail as much as possible.

Additionally, domestic security and law enforcement agencies sometimes share and exchange information with each other, often pursuant to domestic laws,

which permit - and in some cases require - such sharing. Some examples of when public safety and law enforcement agencies may wish to share information include agencies sharing information about fugitives, about convicted pedophiles, as well as information about individuals who pose public health risks, such as individuals who are believed to be carrying a deadly virus.

Domestic security and law enforcement agencies also share information internationally, pursuant to bi-lateral and multi-lateral treaties and other legal instruments. The important concept to bear in mind when thinking about these information sharing mechanisms is that each mechanism should have its own privacy protections built in.

Thus, if privacy legislation or rules are enacted to allow for choice by an individual in relation to the collection, use and disclosure of their personal information, these laws and rules should not allow for the option of choice with regard to information lawfully collected, used or disclosed by law enforcement or domestic security agencies.

Principle 8. Access and Correction

While privacy laws that require information controllers to provide individuals with the right of access to, and correction of, their records are an important component of any privacy regime, there are certain instances when access and correction rights should be denied. One of those situations is when the individual's records are the subject of a law enforcement or domestic security investigation.

Specifically, as part of an ongoing investigation, a law enforcement agency may use lawfully authorized investigative tools, such as a subpoena or a search warrant. Since these legal processes would necessarily be served upon the provider supplying the service in question to the individual target of the investigation, it is not uncommon that a copy of the legal process may be placed in the individual's file with the provider. Moreover, use of an investigative process might also cause the provider itself to generate information regarding the target individual. The customer should not have "access" to this information.

For example, if a production order is served on a provider by a law enforcement agency, asking the provider to produce information from a suspect's E-mail account, it is possible that the provider might somehow note the service of this document in the suspect's account, or otherwise add information to the personal information fields in order to facilitate this legal request. If this individual were then allowed to access his account and personal information, it is feasible that the individual would see the information added by the provider, thereby disclosing an otherwise confidential investigation. Similarly, in response to an individual's request for all documents in her account to be mailed to her, a company may make copies of all documents in the file, including a copy of the

production order served on the provider for that account, again disclosing a confidential investigation.

Privacy laws also need to incorporate exceptions to an individual's right to correct personal information. Allowing an individual to change his or her personal information, under the premise that it is incorrect, when the individual is under investigation for criminal activity would, in essence, allow the individual to cover his or her criminal tracks by deleting or changing the very evidence that an investigator would use to identify and apprehend the criminal.

Take, for example, a kidnapper who signs up for an E-mail account (providing personal information) that the kidnapper then uses to communicate with the family of the kidnapped child. After sending threatening E-mails demanding a ransom for the return of the child (or the child will be killed), the kidnapper calls up the E-mail provider and tells the provider that his personal information they have on file is incorrect, and asks them to alter, or delete it (depending upon the capabilities of the provider).

While the kidnapper is requesting that his personal information be corrected under the premise that it is incorrect, the reality of the matter is that he is really changing it (or seeking its deletion) in order to cover his tracks and destroy evidence available to save the child. Often times, especially in the electronic world, these little pieces of evidence are the only strands of evidence available for catching the criminal and, in this case, saving the life of the child.

Conversely, if the privacy law contained an exception allowing companies to refuse the right of correction when done so because of a lawful investigation, the company could make a note of such investigation on the file and then, when the kidnapper makes a request to delete or change his information, the company could rely upon that legal exception to deny this request.

What this example hopefully illustrates is that when drafting privacy laws that provide for the right of access and correction, it is important to incorporate exceptions into that law for when:

- the personal information has been the subject of legal process that bars disclosure;
- the disclosure of the information would pose a threat to an ongoing law enforcement and/or domestic security investigation; or
- the disclosure of the information could pose an imminent threat of harm or death to others.

Finally, as noted in the commentary to Principle 8, laws should not require an explanation if a company denies a request for access or correction based upon an ongoing investigation or based upon legal process that has been served demanding confidentiality. One question that this raises, and drafters may wish

to consider, however, is how can a company refuse to provide an individual with a reason for denying access or correction without giving away the fact that there is an investigation of the individual or that legal process has been served? In other words, if the only time such denial is done by a company is when there is an investigation, or when legal process has been served, wouldn't the denial of the request, in itself, automatically give notice to the individual that his personal information is the subject of an investigation? We pose this question here so that the drafters might further consider this complex issue.

In summary, what should become clear from these examples is that any time a privacy law mandates companies to provide individuals with access and correction rights, that law also needs to contain exceptions allowing companies to deny such requests when access or correction would compromise a lawful investigation.

Principle 9. Accountability

As discussed previously, voluntary cooperation by private industry is often the lifeblood of law enforcement investigations. Moreover, as the operators of our critical infrastructures (such as power, energy, transportation, etc.), private industry will often be the first to know of threats to our safety and security.

For example, a transportation industry company might receive an E-mail from an employee threatening that a train containing hazardous materials, which is traveling through a densely populated region, will be bombed. The transportation company will, of course, want to take whatever steps necessary to assess the validity of the threat but, in reality, will likely need the assistance of a law enforcement agency in order to evaluate the threat and hopefully prevent the incident from occurring. This would certainly mean that the company would have to be able to report this incident and turn over the E-mail, as well as other relevant records containing the employee's personal information.

According to Principle 9, before transferring personal information to another person or organization, whether domestically or internationally, the personal information controller (in this case the transportation company) would have to "obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles." Since it would not be prudent to seek the consent of the employee in this situation, the company would have to rely upon the second aspect of Principle 9, namely that the company "exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information. . . ."

Yet, unlike business scenarios where private industry might provide personal information to another private entity, a company will not be permitted to review the books, records and information systems of a law enforcement or domestic

security agency prior to disclosure of this personal information. Moreover, due to the imminent threat of injury and death to others, the company would not have the time to conduct such a review even if such a review were feasible.

In short, it is crucial that information controllers feel comfortable sharing this type of personal information with law enforcement and national security agencies, despite the fact that they will not be able to conduct the due diligence they would otherwise conduct before transferring information to another private entity. In order to accomplish this, and to avoid any concerns about litigation being brought against a company for disclosing this information to the law enforcement agency, privacy laws could be drafted to reflect the fact that a transfer of personal information to a law enforcement or domestic security agency cannot be the basis for legal liability. Another way to resolve this issue could be for an economy to adopt a law that creates a presumption that a company has used due diligence in the transfer of information whenever it transfers that information to a law enforcement or domestic security agency.

Of course, there are only two examples of ways to deal with this issue, and there may be many more options available within a given economy. The overarching goal, however, is to ensure that companies feel comfortable voluntarily turning over information to law enforcement and domestic security agencies for the purposes of facilitating public safety, reporting crime, stopping terrorism, etc.