

## ITI PRIVACY ISSUE BRIEF

### SCOPE OF PRIVACY LEGISLATION

A threshold question for any new privacy bill is the scope of activities, information or media it will cover. Past federal privacy laws have applied broadly, such as to all financial institutions or all medical records – as well as narrowly, to things like video rental records or telephone call logs.

The same will be true of bills in the 107<sup>th</sup> Congress, some of which will apply to specific practices and others of which would lay the foundation for a new body of law to govern the relationships between businesses, non-profits and the individuals they serve. A key question to consider is whether broad-based regulation of all Internet-based commercial activity is the appropriate scope for new privacy legislation.

#### ***Some unanswered questions:***

- Does an “Internet-only” bill track the actual threats to privacy and/or the actual causes of public concern?
- Would an “Internet-only” bill distort the market?

#### **ITI’s position:**

Individual privacy concerns are generally not defined by the medium through which personal information is collected, but rather by how sensitive the information is, who has it, and what is done with it. The ideal approach to privacy would, to the greatest extent practicable, apply similar protections to personal information entrusted in both online and offline transactions while recognizing the unique properties of each medium.

#### **Personally information is shared through various channels and an individual’s vulnerability is not limited to “Internet” transactions.**

As technologies and business models converge, individuals make their personal data available through a variety of channels, including the Internet, public telecom networks, private identification and access systems, store automation systems, credit card systems, electronic banking systems, and various non-electronic means. Misuse of personal data can, and does, occur with data received from all of these sources. In fact, several of the most noteworthy compromises have been of consumers’ information obtained from sources other than the Internet. Wisely, the Financial Modernization Act of 1999 and the resulting regulations apply equally to on-line and off-line institutions and transactions.

### **Technology convergence is blurring the “on-line” and “off-line” distinction.**

With many next-generation technologies, it will not be clear whether an individual is “on-line” or not. For example, with some applications, consumers will place phone calls to Internet-connected computers with voice-recognition software, so they are “talking to the Internet.” As the next generation of cellular phones creates a mobile Internet, the distinction between the mobile telecom system and the Internet will become meaningless – data transfer may be on the “Internet” but other information (e.g., the user’s location) will be on the cellular network. Another example of convergence that makes the “on-line / off-line” distinction meaningless is the movement toward “voice over IP.” With this technology, individuals will likely release some personal data to a supplier through traditional Internet data transfer and, during the same transaction, release other PII through a “voice call-through” over the Internet.

### **Unequal regulation of on-line commerce will slow development of the new economy.**

The networked economy is widely recognized as driving the overall US economy, in 1999 growing 15 times faster than the overall US economy and creating 650,000 new jobs. Additionally, networked applications (commercial, educational, financial, medical, etc.) are providing the means for more remote and less-affluent geographic areas across the globe to obtain otherwise unavailable first-rate services. The US government has wisely sought to encourage the development of the “Networked World,” in part through resisting regulation of the Internet. Applying more onerous privacy regulations to the Internet than to other channels of commerce would have the undesired side effects of restricting the availability of services, impeding the development of the “New Economy,” and slowing overall economic growth.

### **OECD guidelines and the EU Directive are applicable to all PII.**

The Organization for Economic Development and Cooperation promulgated the basic framework for handling PII in 1978. Their guidelines do not distinguish between the means by which information is shared, but rather apply similarly to all PII. Similarly, the EU Privacy Directive applies to both on-line and off-line data. The US might not wish to replicate the European Privacy Directive because of its shortcomings. Nonetheless, U.S. companies that have operations in Europe and transfer customer or employee data into the US will be required to observe the regulations for both on-line and off-line PII.

### **RECOMMENDATIONS:**

All users of personally identifiable data should employ sound data privacy principles in the handling of this data, regardless of whether data is obtained through on-line or off-line transactions. To the extent that US legislation or regulation is required to ensure a level of privacy protection to consumers, the resulting regulations should, to the greatest extent practicable, apply similarly to all personal data, regardless of whether it is obtained through on-line or off-line channels.