The Economic and Security Costs of Obsolescent Computer Laws

During the last two decades of the 20th century, several Federal statutes were enacted to adapt the powers of government to investigate and enforce criminal laws and to limit the undetected surveillance capabilities of corporations and third-party service providers. These statutes responded to two significant technology trends: (a) the improved abilities to monitor and record traditional voice communications without the consent or knowledge of any participant, enhanced by improved technologies for storing those communication records, and (b) the capability of emerging technologies for voice and mail communications to bypass the installed infrastructure of traditional copper-wire telephone systems (through the use of mobile telephones and electronic mail systems).

The Electronic Communications Privacy Act (ECPA, enacted in 1986) is one important example, which focused on the ability of government and corporations to employ intercept devices with specified wire, oral or electronic communications, and to access and rely upon stored communication records. At the time ECPA was enacted, federal law enforcement officials were endeavoring to update the functionality of the Wiretap Act (enacted in 1968). The Computer Fraud and Abuse Act (enacted in 1984 and revised in 1994) is another example; Communications Assistance for Law Enforcement Act (CALEA, enacted in 1996) is a third. Collectively, while there was greater awareness of the Internet with the later laws, the legislative language has challenged 21st century computing and communications practices.

Since their enactment, governments, corporations and the courts have struggled to interpret the applicability of these statutes to the rapidly evolving technologies and communication services that have been built upon the platform of the Internet. Many of the critical words used in the 20th century laws have proved difficult to apply to 21st century technologies—key terms such as “intercept”, “record”, “monitor”, “electronic communication”, “contents”, “transmission” were not drafted with a focused capability to adapt to evolving Internet services.

The collisions, conflicts and adverse impact of these laws on business efficiency and competitiveness are now being illuminated by the emergence of unified communications (UC) as a critical new portfolio of Internet-based business services. At a time in which US companies are desperately looking to find new operational efficiencies and improve their competitive capability in a global, wired market, the existing legal issues created by these 20th century laws are inhibiting sound, productive investments in UC solutions. Simply stated, companies are genuinely concerned that they are unable to employ modern, conventional Internet security services across UC solutions without exposing themselves to legal sanctions and possible prosecution.

Unified Communications Defined

Unified communications solutions present a portfolio of amazing diversity, with innovation and imagination continuing to produce new and improved technologies and services. Generally, unified

communication solutions use Internet systems and networks to integrate the full-range of communication mechanisms (voice, video, data, text) and deliver to organizations and individuals improved efficiency and operational effectiveness. Unified communications include, but are certainly not limited to:

- Voice over IP (VoIP) services, allowing voice communications traditionally carried on PBX -wire or cellular systems to be transmitted and delivered over the Internet.
- Integrated messaging, allowing the content of voice mail, electronic mail, instant messaging or text-based communications to be converted into alternative formats.
- Multi-media services, delivering video, voice and integrated messaging on an integrated service platform.
- The use of technologies to forward communications to multiple locations (network, desktop, portable device, home computer) creating an ability of users to enable their "presence" to be improved, thereby dramatically reducing delays in business processes provoked by travel, availability and similar variables.

Securing Unified Communications

Consistently, the introduction of new Internet technologies attract opportunists, hackers, sophisticated criminal networks and others that undertake malicious activities to disrupt the technologies, or use the new solutions to obtain unauthorized access to proprietary systems, data or services. The real-time, high-availability aspects of VoIP and other unified communication services create a range of security risks that must be combated effectively in order for the services to be viable and effective.

Here are some of the security risks that the Internet Security Alliance and others have associated with the use of these services and technologies:

- The creation of denial-of-service attacks that exploit the structure and format of the UC communications and formats to disrupt network availability.
- Hijacking of calling numbers or services, in order to misuse a VoIP network or service to impersonate authorized users and make unauthorized calls or conduct improper communication sessions.
- The creation and use of commercial spam over Internet telephony (known as SPIT).

In addition, since most unified communication services transmit and receive content using Internet protocols, many long-recognized security risks presented by the Internet persist with these new services (such as malware embedded in disguised IP messages). UC communications are just like any other IP messages—they are a structured package of data packets. In order to protect against malware and other malicious conduct, the packets must be captured, filtered and analyzed. However, these essential

Internet security services are considered to potentially collide with laws regulating "interception", "monitoring", access to stored content and other restrictions expressed in 20th century computer laws.

The Economic and Security Costs

Despite the enormous economic and competitive potential of UC technologies, genuine and serious issues exist as to whether the 20th century laws prevent corporations from employing conventional and effective Internet security practices which protect their networks, computers, data and business partners against malicious and criminal misconduct. As a result, unable to apply security controls:

- Corporations are withholding their investments in UC solutions; doing so inhibits their ability to access increased operational efficiencies offered by UC technologies.
- Businesses are limiting their use of UC solutions in order to not permit any Internet activity against which existing, effective security controls can be employed. This limits the availability and use of various third party services, and thereby also increases the implementation costs (as a general matter, internally installed UC solutions are more expensive than Internet-based solutions provided by third parties).
- Business networks—customers, suppliers and service providers creating communities and markets through the Internet—are handicapped from integrating UC solutions into their operations because of the inability to secure the Internet-related traffic.

In addition, regulations and interpretations of existing laws proposed during the final months of the Bush administration suggested that, since UC solutions empower normal companies to be able to provide the same services as Internet telephony, any company operating the UC-related servers and routers would be considered as a "communication common carrier", subject to the investigative and warrant powers of the Federal government (as well as minimum technology standards that enable expedited access and monitoring by Federal authorities of the related communications). The specter of potential Federal investigatory powers being imposed on any company offering UC solutions, even for internal use, has further handicapped the appeal of these new technologies.

It is inconsistent with new Federal policy to stimulate the economy to allow 20th century computer laws—and the risks of prosecution or unacceptable intrusion into corporate networks—to inhibit the availability of new technology solutions that enable American companies to realize new efficiencies and competitive advantages. Applying sound, conventional security controls to any Internet-based packet traffic should not be the basis for potential Federal legal action. Instead, the legal framework must be reviewed, and revised, in order that strong, consistent corporate security practices can be employed. The end point should not be an abandonment of the important policy interests served by ECPA, CALEA and other 20th century laws; instead, a different balance is required that enables public-private sector partnerships to expand and mature in order that security activities may properly focus on the truly bad actors that threaten the integrity and operations of American networks and challenge our collective cyber security investments.

The Response of the Internet Security Alliance

In December 2008, the Internet Security Alliance commissioned a study to evaluate the interactions among existing security services, UC solutions, and existing laws, regulations and commercial practices. This study is intended to produce an authoritative, objective analysis of the applicability of 20th century legal rules to 21st century unified communication services and the uses of existing security controls.

The members of the Internet Security Alliance are working closely to inform this legal/technology study. To conduct the study itself, we have commissioned Jeffrey Ritter, Esq. of Waters Edge Consulting. Mr. Ritter has had a distinguished legal career in contributing to the advancement of online commercial practices and, as well, the development of strong information security practices that align with domestic and international law.

Our legal study is intended to be completed in the second quarter, with a working target date of April 30. The study is intended to produce several useful deliverables:

- An objective and thorough analysis of the existing laws, regulations and case law potentially affecting the use of effective security technologies for unified communication services.

- Recommendations on how to navigate potential conflicts or uncertainties between existing law and security technologies through the constructive use of different policies or procedures, commercial practices or contracting language.

- Possible reforms to consider, whether through legislative action or agency rulemaking, that will eliminate any conflicts or uncertainties that cannot be navigated through commercial practices. These potential reforms, if needed, would certainly be useful in facilitating a more flexible legal framework for existing and future Internet-based services. To be clear, we are not advocating to abandon the important policy considerations behind existing law; instead, we are concerned the laws themselves require a more nuanced alignment to enable 21st century security to be fully effective for all stakeholders in the future security of the Internet.

We want to encourage the Administration to be fully apprised of this important project. Of course, as the project reaches completion, the Internet Security Alliance will share our report and recommendations with the Administration. We look forward to having the opportunity to provide more detailed briefings or information, and to make available our members and experts to your deliberations.