Navigating Compliance and Security for Unified Communications

This publication is for informational purposes and is not a substitute for legal advice. The information in this publication should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. It is intended for use by corporate legal counsel, other corporate officers or managers working with corporate legal counsel or other lawyers. This publication is not intended as, and should not be relied upon, as the practice of law.

Participation in the development of this publication does not represent an endorsement of the content of this publication on the part of any specific company or corporation. Any reference made to existing commercial products or services is not intended as, and does not constitute, an endorsement or approval of such products or services.

While reasonable efforts are made to assure the accuracy and correctness of the content, as of the date of publication, the publication and its distributors make no other warranty or representation.

This publication is protected by copyright, all rights reserved. The scanning, uploading and distribution of this book by electronic means, including the Internet, without the permission of the Internet Security Alliance, is illegal and punishable by law.

If you wish to acquire printed copies of this publication, or distribute portions of this publication in any media, please contact Internet Security Alliance by calling (703) 907-7799.

© 2009 Waters Edge Consulting, LLC. All rights reserved.

Navigating Compliance and Security for Unified Communications

Board of Directors

Larry Clinton
President, Internet Security Alliance

Ty Sagalow
ISAlliance Board Chair,
Executive Vice-President and Chief Innovation Officer, Zurich North America

Mike Hickey
First Vice Board Chair
VP, Government Affairs & National Security Policy, Verizon

Dr. Sagar Vidyasagar
Second Vice Board Chair
Executive VP, Advanced Technology, Tata Consultancy Services

Marc-Anthony Signorino
Secretary/Treasurer
Director Technology Policy, National Association of Manufacturers

Bruno Mahlmann
Vice President, National Security,
Perot Systems Corporation

Ken Silva
Chief Technology Officer, Verisign

Charlie Croom
Vice President, Cyber Security Strategy,
Lockheed Martin

Joe Buonomo
President, Direct Computer Resources, Inc.

Jeff Brown
Director, Infrastructure Services and CISO
Information Technology, Raytheon

Lawrence Dobranski
Leader, Advanced Security Solutions Research & Development, Nortel

Eric Guerrino
Managing Director Systems and Technology, Bank of New York Mellon

Dr. Pradeep Kohsla
Dean, School of Engineering and Computer Sciences,
Co-Director – CyLab, Carnegie Mellon University

Tim McKnight
Vice President & Chief Information Security Officer,
Northrop Grumman

The views expressed in this publication do not necessarily reflect the views held by any individual member of the ISAlliance Board or Executive Committee nor the companies by which they are employed.

WHAT IS THE INTERNET SECURITY ALLIANCE?

Virtually every corporation integrates use of the Internet into their business plan. However, the use of the Internet also exposes corporations to continuing and persistent threats, putting at risk corporate intellectual property, business operations and overall enterprise security. These risks confront any business, as well as all of their respective suppliers, business partners and customers.

The Internet Security Alliance (ISAlliance) is a non-traditional trade association that serves to understand, integrate and help manage the multi-dimensional and international issues that operating in the Internet age creates. The ISAlliance website is www.isalliance.org.

WHAT DOES THE INTERNET SECURITY ALLIANCE DO?

ISAlliance provides tangible benefits to its membership by creating cutting edge services and applicable publications useful across the various industry sectors that use the Internet. ISAlliance was conceived in conjunction with Carnegie Mellon University to integrate emerging technological issues with the membership's pragmatic business concerns and align public policy to facilitate business growth and resilience.

The ISAlliance provides a broad range of ongoing technological, business and policy services to its membership, all of which can be reviewed in more detail at the ISAlliance web site. In addition, the ISAlliance Board identifies a select set of priority projects each year for intensive work.

This report is a new contribution to a continuing series of publications produced by the ISAlliance that address the substantive issues that arise at the intersections of business, law and information security. Previous titles include:

> The Cyber Security Social Contract: A Twenty-First Century Model for Protecting and Defending Critical Technology Systems and Infrastructure
>
> The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask
>
> Contracting for Information Security in Commercial Transactions, Volume I: An Introductory Guide
>
> Contracting for Information Security in Commercial Transactions, Volume II: Model Contract Terms for Certified Information Management Systems
>
> Common Sense Guide for Senior Managers: Top Ten Recommended Security Practices

Copies of these publications can be obtained or purchased from the ISAlliance.

About Waters Edge

Waters Edge is committed to enabling companies and organizations to develop and maintain trusted digital information assets, through rigorous, objective analysis of how to integrate business, legal and technology management strategies and tools. Further information is available at www.wec-llc.com.

Waters Edge researches and produces analytical solutions for specific client engagements. In addition, for lawyers, paralegals, information security professionals, records managers, IT executives and compliance officers, Waters Edge produces in-depth training courses and comprehensive publications for improving how to create and manage digital information assets. Those courses and publications are part of the CastleQuest Discovery Library, available at www.cqdiscovery.com.

Waters Edge was founded by Jeffrey Ritter, Esq. Jeffrey is recognized as one of the leading voices on navigating the complexities at the intersections of law and information technology in the 21st Century. He was the Founding Chair of the ABA Committee on Cyberspace Law, worked extensively in contributing to the formulation of the essential legal frameworks for online commercial practices, and is widely recognized in the records management and information security fields for his advocacy of using technology and management systems to address legal risk and compliance.

He has previously served as outside counsel to the Information Systems Security Association and is a regular moderator for online conferences conducted by the Internet Security Alliance, ISSA and other leading information security associations.

Jeffrey is a frequent keynote speaker, lecturer and author. He may be reached by e-mail at jeffrey@wec-llc.com or 703.912.6180.

Table of Contents

This Report consists of the following parts, together with a Glossary and Appendices, as listed below. Detailed content listings are included at the beginning of each Part:

Introduction

In 2008, the Internet Security Alliance Board of Directors authorized a project to develop a set of technical materials, in cooperation with the National Institute of Standards and Technology, for improving the security available for Voice over Internet Protocol (VoIP) services. The project's target is the production of a Security Content Automation Protocol (or SCAP) to enable automated vulnerability management, measurement and policy compliance for VoIP services. That project is a major initiative of the Internet Security Alliance and, as of May, 2009, work continues to progress against a defined timetable.

In parallel to the SCAP project, participating corporate members expressed interest in sponsoring a separate project to better understand compliance and legal issues that may be associated with VoIP services and a broader range of unified communication services. Interest existed in evaluating whether legal concerns may be restraining companies or service providers from fully deploying conventional Internet security services with respect to VoIP and other unified communication services and, if so, to develop recommendations on how those legal concerns may be addressed by vendors, suppliers and customers in commercial practice (and with possible legal reforms). The legal research project was authorized by the Internet Security Alliance Board in December, 2008 and Waters Edge was commissioned to conduct the project. This Report is the resulting work product.

Report Scope and Objectives

In undertaking the work, several objectives were established which have shaped the scope of this Report:

- The Report is intended to be a pragmatic, useful resource to companies that are both suppliers and customers for unified communication services, with a special focus on meeting the needs of in-house legal counsel asked to evaluate the legal suitability of employing unified communications in their business. As such, the Report:
    - describes the existing technologies of unified communications (UC) and, in particular, relevant technical aspects that are useful to understand in conducting a legal analysis (*see* Part I—Understanding Unified Communications).
    - delivers an overview of how UC solutions confront Internet security risks and some of the essential Internet security services that can be used to protect a company, its facilities, its properties (including business data) and employees and agents (*see* Part II—Internet Security Services).
    - provides an inventory of relevant laws to be considered in launching and operating unified communications products and services (from the customer's perspective), emphasizing domestic (United States) laws, notably the Electronic Communications

Privacy Act and the Stored Communications Act (collectively referred to as ECPA). That inventory presents a detailed analysis of ECPA and its terms (*see* Part III-The Legal Landscape).

- delivers a detailed analysis to enable lawyers and their clients to evaluate whether ECPA creates legal barriers to the corporate use of relevant Internet security services in connection with UC products and services. (*see* Part IV—The Legal Analysis).

- includes a practice toolkit of recommended practices and checklists for lawyers and their clients to better assure that the use of UC solutions and services does not produce unexpected legal exposure or risk (*see* Part V—Practice Toolkit).

- presents a Glossary (defining key technical and legal terms used in the analysis) and a Legal and IT Resource Inventory, providing bibliographic references to the key legal and technology resources we consulted in preparing this Report. Our reliance on those resources, and additional comments on our research, are included in the Research Notes at the end of this Report.

- In producing the Report, we were asked to also evaluate possible reforms in statutes, regulations or policy that would better enable Internet security services to be employed in connection with UC solutions and services. Those recommendations have been separately delivered to the Internet Security Alliance.

Excluded Topics

Companies conducting business in the 21st century are challenged by a global digital marketplace in which nations and states continue to try to maintain the relevance of 20th century legal systems while concurrently enacting new laws and regulations responding to the social and economic risks, and potential rewards, presented by 21st century technologies.

In many countries, including the United States, courts also struggle to adapt older laws and legal principles to the challenges created by the tremendous capabilities of computing, networking, mobile devices and the rising economic significance of digital information as a new class of property to be created, bought, sold, stolen and destroyed. Taken as a whole, on a global basis, the legal landscape is dynamic and, with particular attention to cybersecurity topics, significantly influenced by major political forces and concerns.

UC products and services potentially collide against many different laws and regulations. In order for this Report to be functionally useful, some decisions were taken to exclude detailed analysis of certain topics, as follows:

- The Report does not examine specific privacy laws outside of the United States that may apply to the communications or records created in using UC products and services. For example, European and Canadian privacy laws originate from very different principles than the privacy laws in the United States. As a result, many different factors can limit the rights of an operator

of a UC product or service from accessing or monitoring certain communications (for example, the personal communications of an employee) originating or transported through Europe. The Practice Toolkit includes a checklist of relevant topics relating to privacy, but no controlling guidance is offered. While we are not generally aware of any European legal constraints on the use of Internet security services to protect against the risks associated with Internet use (as described in Part III), further expertise in the privacy laws of specific jurisdictions may be required to support the implementations of any specific company.

- Many states in the United States enacted "consent-to-record" laws (primarily during the 1980s). These laws are non-uniform and have been inconsistently applied, with varying results. There is also some justified legal grounds to believe that federal laws, notably ECPA, pre-empt the applicability of the "consent to record" laws to anything other than intrastate calls with a specific state. Since (a) we could reasonably find no cases considering the use of security practices under the "consent to record" laws, and (b) the technical feasibility of applying "intrastate" laws to Internet communications is largely infeasible, we have not examined these issues in detail. However, Part III-The Legal Landscape does provide an overview of the state consent-to-record laws themselves.

Despite these exclusions, the Report is believed to be the most detailed analysis to date of the applicability of current federal law to the use of Internet security services to protect UC solutions and services and, therefore, substantially advances toward the original objectives. Of course, all comments, criticisms and suggestions for improvement are welcomed.

Acknowledgements

This Report has benefitted from the time, knowledge and contributions of many formal and informal contributors:

- First, the Internet Security Alliance staff, notably Larry Clinton and Barry Foer, have provided invaluable administrative and substantive support.

- Second, additional Internet Security Alliance members and participants in the SCAP Project have volunteered to participate in interviews that discussed their uses of UC products and services, security and legal issues they have considered, and implementation strategies that have been employed.

- Third, additional expertise and perspective, including that of Jim Dempsey, Esq., Center for Democracy and Technology, and Tom Smedinghoff, Esq., a partner at Wildman Harrold and one of this country's most distinguished authorities on information security and the law, have been welcomed in assuring the focus and integrity of our analysis.

- Finally, special recognition to my colleagues at Waters Edge, David Gaston, Esq., Director, and Shawn Shook, a law student at George Mason University School of Law, for their legal research and review in support of this Project.

Nevertheless, despite the contributions of these other professionals, this work remains the work of Waters Edge and any errors or omissions are those of the authors.

Jeffrey Ritter, Esq.
Waters Edge Consulting, LLC
May 20, 2009

Part I—Understanding Unified Communications

Table of Contents

Introduction

Technology innovations often defy the boundaries imposed by precise definitions. Unified communications (UC), when viewed as a single portfolio of solutions, deliver exciting and compelling functionality and enormous business value. Unified communications offer a cornucopia of solutions that are blurring the distinctions between audio, video and data networks. Some view the emergence of UC as a development as profound as the Internet itself.[1] UC solutions facilitate the integration of corporate networks, business communities and market systems, eliminating the need for separate network structures (such as phone systems, cell phone systems, data networks, video networks) that require extensive technical support to enable content migration.

[1] "These are exciting times. When we look back in five or seven years, we're all going to say, 'Wow! There was never was a category this big that went through such incredible change in such a short time. It's like the mainframe-to- PC revolution all over again, or the emergence of the Internet. It doesn't get any more exciting than trying to look ahead and figure out what the world of UC is going to look like. We'll all be surprised when it all plays out." Kevin Gavin, Vice President of Marketing for ShoreTel, quoted in Grigonis, "Year-End Review and Future Trends in UC" (Unified Communications Magazine, November, 2008), available at http://hdvoice.tmcnet.com/topics/unified-communications/articles/45576-year-end-review-future-trends-uc.htm.

Highlighting the newness of the field, extensive research failed to discover a single definition of UC that had been accepted in the marketplace. Unified communications is perhaps best defined by examples, rather than by a singular definition, but doing so requires some care. The enthusiasm of solutions providers to identify their products with a popular innovation in the marketplace—"marketspeak"—overstates the number and range of solutions parked under the "unified communications umbrella". However, as discussed later in this Part I (The Technology Architecture—How It Works), "true" unified communications solutions share a common technology foundation that limits whether a particular product or service is a "true" unified communications solution. Nevertheless, the range of unified communications solutions ("UC solutions") is surprisingly diverse.

UC solutions (as of May, 2009) generally include the following solutions, organized into two bundles. The first bundle emphasizes the movement of communications across different media and formats, while the second bundle emphasizes unifying communications with the concurrent use of other business applications.

Unifying Communications Media

- *Instant messaging (or "IM")*—delivers informal text-based conversations among two or more participants (also called "chat"). Most IM technologies allow a single user to conduct concurrent, multiple IM sessions with different conversation partners. IM technologies enable users to transmit digital files, attachments, links to websites, stored digital images and live video transmissions during an IM session.

- *Voice over IP (or "VoIP")*—enables voice conversations to be conducted, for which some or all of the conversation is transported across Internet networks and devices (rather than conventional "plain-old-telephone-service" (also known as "POTS"). The conversation content is digitally converted into digital packets that are routed and managed together with other Internet-based data and content pursuant to Internet protocols (hence the term "Voice over IP" or VoIP). Users generally employ headsets connected to the computer (or microphone/speaker combinations) to do so, but traditional handsets are increasingly used, making VoIP calls indistinguishable to the average person making or receiving a call.

- *Video*—delivers video (with or without sound) separately or concurrently with other content. For example:

    - A small camera installed on a computer can transmit a video image of the speaker during a VoIP session or IM session.

    - A computer-installed camera can transmit a speaker's video image and sound while the speaker is transmitting and displaying another application (such as a text document or slide presentation).

- *"Presence"*—a combination of technologies and software applications that allow a single user to control the phone or other device (computer, cell phone, laptop) to which any inbound

communications are forwarded—this enables the user to maintain their "presence" despite being away from their assigned location, moving between locations, or conducting business from a client office or facility. The user is instructing the technology to "find me—follow me" in order to allow the user to receive and respond to communications. "Presence" solutions offer a range of options across different vendors and technologies:

  - A user can eliminate maintaining multiple phone numbers and have a single number at which she can be reached; the UC solutions allow the user to provide instructions at any time specifying the phone or device to which an inbound call is to be forwarded.

  - A user maintaining different roles (sales director, audit committee, strategic planning) can, based on their roles, selectively be "in the office" only for communications directed at the roles the user selects, and "out of office" for other communications.

  - Similarly, a user can selectively be "in the office" only for those in-bound callers (or roles) the user may designate.

- *Message Media Conversion*—delivers the option for messages transmitted or recorded in one media format (such as text or voice) to be converted into another media format:

  - *E-mail to Voice*—E-mail content is synthesized by technology into an audio recording in which a computer-generated voice "reads" the e-mail aloud. This allows the user to access their e-mail through their voice mail system.

  - *Voice to E-mail*—A voice mail recording is analyzed and converted into a text-based message, which is then delivered like an ordinary e-mail. This allows the user to access their voice mail through their e-mail system.

  - *Embedded Voice Mail*—A voice mail recording is stored as an embedded digital object inside a normal e-mail. This allows the user to directly hear the voice mail without traditional telephone access.

  - *Fax to E-mail*—An image of a document received by fax is automatically converted into an attachment to a normal e-mail, allowing immediate access to the fax image.

Among the various impacts of these innovations, the preceding have the practical effect of migrating to a telephone device, particularly hand-held mobile units, many computer functions, and, in turn, enabling computing devices to serve the communication functions of a traditional telephone.

Unifying Communications with Business Applications

A second bundle of UC solutions address the situation when a participant in a real-time communication (IM, voice, e-mail, etc.) must separately open a business application for additional communication activities (e.g., reviewing a spreadsheet) and not be able to "unify" the activities. Inefficiency, and the potential for errors, are a frequent consequence, tolerated until now as ordinary business process. UC

solutions enable a more agile, integrated approach, allowing the different applications required for communications and business to be operated more coherently; Gartner calls the results "communications-enabled business processes"[2]. For example, UC solutions allow:

- A telephone number displayed on a web page to be dialed directly (using VoIP) by clicking on the number within the web page, without separately opening up the required software application.
- Two people viewing concurrent videos of each other from their computer cameras to also view and share an application operating solely on the computer of one participant.
- A conference call to be convened, in which all participants connect through VoIP and then can conduct concurrent IM/chat sessions with different participants, all within the same application.

The Compelling Business Case

UC solutions offer, and deliver, a compelling business case for improving the efficiency and productivity of every connected enterprise resource: computers, devices, networks, data and people. By employing technology to connect and unify the availability of communication content, the solutions overcome persistent issues in business that have persistently blocked organizations from realizing the full potential of existing technology to improve the agility, responsiveness and effectiveness of the enterprise. UC solutions address:

- *time delays caused by personnel travel, mobility and inaccessibility*. By routing content to the preferred devices, and by converting content into the most acceptable format for a specific employee at any given moment, companies are able to dramatically reduce delays that had otherwise been tolerated.
- *accuracy and time delays caused by manually converting or transferring content between media*. For many employees on the go, accessing communications content has often relied on assistants, clerks or other team members to forward the substance (e.g., leaving a voice mail "You received an e-mail from the CEO to call him"), or transfer the content (e.g., sending an e-mail into which the text of a fax has been manually typed). UC solutions eliminate these practices, and enables rapid, accurate delivery, without the potential for errors or associated time-delays.
- *inability to prioritize access or availability*. For many executives and managers, technology has eliminated the traditional "gatekeeper" role of an executive assistant or secretary. UC solutions empower the user to construct and operate their "gates" directly, controlling availability and access based on priorities, roles and other variables that software applications offer.

In delivering those benefits, UC solutions directly draw into question the continued investment and operating costs for POTS. Those costs can be substantial, both in terms of direct expenses incurred for

[2] Id.

third-party services and support, as well as the internal resources assigned to acquire and operate internal phone networks and providing administrative support (e.g., calculation of charges, equipment management and replacement, etc.). For many companies, eliminating these costs, and migrating all of their communication activities onto an Internet-based UC platform, offers a compelling proposition, particularly in economically challenging times.

The Technology Architecture—How it Works

UC solutions share a common technology foundation with several distinctive elements. To best understand these elements, it is useful to briefly review the technology architecture of the communications networks and systems that UC solutions replace. Understanding the technology is invaluable to also understanding why existing laws have many of their features (as discussed in Part III—The Legal Framework), and some of the resulting tensions between those laws and the wide-ranging commercial uses of UC solutions in the marketplace.[3]

20th Century Communication Technology

POTS remains a dominant infrastructure component of developed economies. Physical, wired networks criss-cross our world, providing the medium through which voice calls, faxes and data transmissions can be accomplished. The wiring itself has changed over time, with copper wiring increasingly replaced by fiber-optic cables, and satellites replacing major network switches. As a result, except for local service (sometimes referred to as "the last mile"), much of the infrastructure through which POTS is delivered across North America and many other regions consists of a complex, robust infrastructure of digital components.

Each telephone call that is initiated calls upon the POTS network to establish a circuit, connecting the telephone device from which the call is initiated to the device (as represented by its telephone number) to which the call is directed. The circuit can be established, by example, between:

- Two persons conducting a conversation.
- One fax machine transmitting to another machine (for which there is a separate signal sent to establish the connection across the circuit).
- Two computers transmitting data.

Through interconnection agreements and services, a circuit can be established across the networks of multiple public and private communication carriers. Once established, the circuit is maintained for the entire duration of the communication. This unitary function of a POTS circuit, connecting one telephone

[3] This technology discussion supports the subsequent analysis of this Report, but is not offered as a complete or full technical discussion of either existing POTS technologies, or the full features and functions of the varied UC solutions. Appendix 2--Legal and IT Resource Inventory includes references to numerous additional public websites and publications that can be accessed online for more detailed analyses.

device to another for the entire duration of a call, is important to understanding how certain federal laws are structured.

At the basic level, traditional POTS circuits are best known as the familiar "land lines" used in homes for one-to-one communication. While a single home telephone may only be able to support one circuit at a time, companies may acquire PBX (private branch exchange) switches that allow multiple circuits to be concurrently opened and maintained, and allow inbound and outbound calls to be routed and managed across multiple extensions within the company. Trunk lines, high-capacity lines capable of carrying very large numbers of circuits, connect to make up the backbone of our POTS systems.[4] At the switches between local connections and these networks, a voice communication (an analog signal[5]) is translated into a digital signal that is carried across the backbone and then re-translated back into analog format prior to the receiving end. Complex signaling technology is employed to assure the quality of the analog signal (in order that the receiver hears something similar to what was spoken by the transmitting party; in the absence of good quality, we experience "a bad signal").

Cell phone technology converts the signal of a telephone call into a radio transmission. For each call, two frequencies are employed, one for sending and one for receiving. The call content is converted from analog to digital and the receiving device captures and decodes the content, reassembling the content into a unified signal that sounds like the voice we are intended to hear. Devices are assigned electronic serial numbers (ESNs) that are cross-indexed to the more traditional telephone numbers we employ; each device is constantly transmitting a radio signal to the networks in order to communicate its location.[6] When a POTS call is initiated to a cell phone, the circuit is established to the cell phone provider's system, which, in turn, converts the voice/analog signal and transmits the signal by radio to the cell phone.

When compared to the Internet, and UC solutions, the distinctive feature of POTS services to emphasize is the fact that, historically, an exclusive circuit was established between two users for the duration of a telephone call or data transfer session. The two end-points of each session could be identified, the circuit could be isolated and, for law enforcement purposes, the content of the conversation could be accessed in real-time by attaching undetected a device that could monitor and/or record the conversation (hence, "wire-tapping"). This technology feature was important to how 20th century laws involving wiretapping and surveillance were eventually formulated (see Part III-The Legal Landscape).

The Internet and Unified Communications

The Internet, as a communications infrastructure for business, remains less than 20 years old. Despite its ubiquitous presence in our business and personal lives, we often overlook its relative youth. The

[4] Satellites further expand the ability of transporting very large volumes of circuits among physical, wired networks.

[5] See the Glossary of Defined Terms for a definition of "analog signal".

[6] This radio send/receive function is now being relied upon for a range of practical uses—locating the nearest restaurant, finding nearby friends, recording and tracking bicycle rides, etc. It also can be a source of information that various UC solutions may employ (e.g., when my cell phone is on, and I am at home, as defined by a specific geographic reference communicated by the radio signal from my cell phone, take voice mail for all calls).

compelling daily utility of the Internet also invites us to overlook the significant challenges that continue to be presented—challenges that involve functional security, the protection of corporate property, the privacy of individuals and businesses, and the powers of government to investigate and suppress illegal conduct that is hostile to society's best interests. It is easy to forget that the Internet is still evolving from its origins as a technology designed to enable continuous military communications toward becoming the indispensable means by which a very substantial portion of recorded information generated by the human experience is created, transported, maintained and stored, whether in business, personal life, government or the arts.

Internet technologies diversify at an astounding rate. The worldwide breadth and accessibility of the Internet has fueled this growth, creating new players in the global business and technology community and providing incredible competitive opportunities. In this environment, UC solutions represent a significant new step toward empowering digital content to be flexible and adaptive, available to users through a wide variety of Internet-based tools, software applications and utilities. UC solutions do so by creating and transporting content through a shared functional characteristic—the capacity to transport content in digital packets during a session.

Understanding Packets

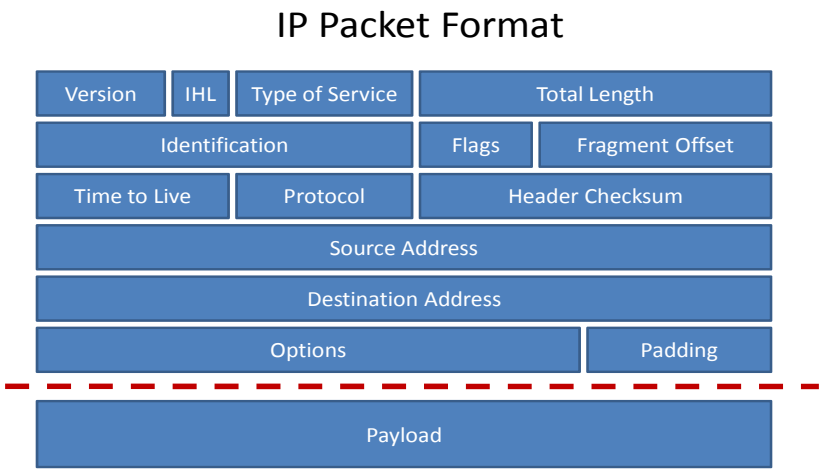
The Internet delivered a fundamentally different means of communicating data, when compared to the circuit-based POTS system. Instead of transporting content in a single, uninterrupted stream (the format employed for POTS calls), the content (such as the text of a message or a voice communication) is divided into packets. The Internet is referred to as a packet-switched network, and the packets are transported and processed pursuant to a set of standard protocols, referred to as the Internet Protocol (or IP) suite.[7]

To enable the effective routing of content, each device connected to the Internet is generated and assigned an IP address, a unique identifier that is recorded and recognized across the Internet. Once a specific content object is divided into packets, the packets are then transported across the Internet to their destination (a specified device to which an IP address has been assigned); however, in contrast to a single circuit, Internet technology allows the packets of different messages to be co-mingled with the packets of other messages across the different networks travelled by the packets.

In fact, different packets within a message may be transported across the Internet via different routes, and across different networks, operated by different service providers. The Internet is, in this respect, location insensitive—based on the most efficient path between two IP addresses, specific traffic may be routed across national boundaries, only to return to the nation from which a message originated, even if the message is only being transmitted between next door neighbors.

[7] *See, generally,* The TCP/IP Guide, available at www.tcpipguide.com. This resource provides simplified but generally reliable explanations of many of the IP architecture topics; of course, many other sources exist that explore in depth the IP standard protocols, notably the publications of the Internet Engineering Task Force, located at www.ietf.org.

One of the inherent architectural features of the Internet is that it provides alternative available paths between destinations; in the event a particular path is not available (due to a technology failure, data volume or similar factors), the routers will find an alternative path.[8] The receiving device receives and re-assembles the data into a coherent structure, and uses various messages to communicate to the sending device that the data has been completely received.



To enable this functionality, each packet is constructed of the following elements (see above illustration[9]):

- A header, which provides a detailed inventory of information required to transport and re-assemble the overall message, including:
  - the type of service a message represents (such as e-mail, data or other services).
  - the total length of a message.
  - identification information, including the source IP address and the destination IP address.
- The payload, specifically that portion of the content of the message included in the packet. For UC solutions, examples of the payload content may be:

[8] This feature was similar to the original design strategy for the Interstate highway system in the United States. Both systems (the highways and the Internet) were designed to offer alternative transit paths, in the event one route may be blocked or disabled (this feature is often referred to as "routing around failure").

[9] This image is based on RFC 791, published by the Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc0791.txt.

- the text of an instant message.
- a digitized portion of an oral conversation being conducted through VoIP.
- a video segment.

Source devices and destination devices engage in rapid negotiations and dialogues to confirm that a message (and its packets) can be received, that packets are being received, that no packets are lost or rendered unreadable during transmission and that a transmission is complete. Similar negotiations and dialogues occur across all intermediate routers and other devices that route the messages between their source and destination.

As most Internet users experience at one time or another, Internet-delivered content can still occasionally not be received as it was intended. In most instances of unsuccessful transmissions, represented by lost or garbled packets, the content is re-transmitted and received automatically, with no visible delay to the users. In other instances, delays may occur. In such cases, the content awaiting transmission is stored at the server level, until the transmission can be completed. Rarely, the entire message is never received, in which case the original message is re-transmitted, or the sender is notified of the message failure.

The occasional delays create no real disruption for Internet users when the content is an electronic mail or a routine data transfer between business applications. However, when IP protocols and packet technology were considered for communicating voice and other real-time dependent applications, those delays were unacceptable. Portions of voice conversations would be lost, creating dead silences or garbled, broken transmissions; similar results occurred with video and similar content when conventional IP addressing and packet switched services were employed. So, to pursue the full potential of the Internet to transport those additional types of content, new solutions were pursued.

Understanding SIP (Session Initiation Protocol) and RTP (Real-Time Transport Protocol)

Two Internet standards work together to provide the essential technical structure which enables unified communications solutions—SIP (Session Initiation Protocol) and RTP (Real Time Protocol).

SIP—SIP is a protocol through which Internet-connected devices initiate, maintain and conclude a session.[10] SIP provides four basic functions:

- SIP establishes a user's location.
- SIP provides for feature negotiation, allowing users (and their devices) to select and authorize the features to be supported during the session.

[10] The formal SIP specification is IETF RFC 3261, issued in 2001, available at http://www.ietf.org/rfc/rfc3261.txt. Additional IETF specifications address enhanced functions—rules to locate SIP proxy servers, resolve error codes, provide for the reliability of server responses, etc. *See* http://www.sipcenter.com/sip.nsf/html/WEBB5YNVK8/$FILE/Ubiquity_SIP_Overview.pdf (last visited April 22, 2009).

- SIP allows the selected features to be changed while a session is in progress.

- SIP is a mechanism for call management—adding, dropping or transferring participants.

The SIP protocol allows a device to communicate a session request to the destination device; the information included is very similar to the information used for web-based browser communications (well-recognized as the "http" format used with web page addresses). A related protocol, the Session Description Protocol (SDP), communicates additional information regarding the media type to be employed during a session, the format(s) and other parameters. However, once a session is established, the content of the session is transported using the RTP.

RTP—RTP is a standard to enable the packet-based transport and delivery of multi-media content. RTP specifies the standardized packet format (both for header and payload) to be employed for audio and video content. Using RTP, applications and devices avoid the risks of garbled or spotty content transmissions, and enable the "streaming media" delivery of audio and video content with which so many web-enabled Internet users have become familiar by sequencing and timestamping the packet data.[11] In a VoIP session, two RTP streams exist, very similar to the circuits employed with POTS. RTP is not required for text-based sessions, such as IM, but is standard for any audio or voice-based media content transmitted during a SIP session.

Note: SRTP (Secure Real-Time Transport Protocol) is a companion standard that enables an RTP session to be protected with encryption, message authentication and integrity. At a practical level, a SIP session conducted with SRTP achieves for the end users the same functional effect as a POTS circuit—the end-users have an expectation of privacy not unlike the expectation of those who use POTS for normal telephone conversations. However, with SRTP, each packet is secure, as compared to a fully secured Internet circuit (which is commonly known as a virtual private network (or VPN[12])).

These protocols were developed in order that the communications can be transported as part of the layered communication protocols that enable the Internet to operate effectively. Each "layer" provides certain functions that enable the other layers to interoperate. For example, the TCP/IP model includes four layers:

- *Applications layer*—which includes the protocols allowing applications to exchange data.

- *Transport layer*—which facilitates end-to-end data transfer, allowing multiple operations to occur simultaneously.

- *Internet layer*—which addresses the addressing, packaging and routing functions are implemented.

---

[11] *See, e.g.,* http://www.cs.columbia.edu/~hgs/rtp/faq.html (last visited April 22, 2009).

[12] Generally, a VPN employs security controls such as encryption to increase the confidentiality and security for specific Internet-based communications. The Internet Engineering Task Force has produced a series of protocols for VPN processes (such as RFC 2547 and RFC 4026). *See, generally* www.ietf.org.

- *Network access layer*—which enables the packets to move on to a network and from a network medium.

These different layers must be successfully navigated by any solution, and adhering to the specific relevant protocols is essential in order to be successful.

Taken together, SIP is the fundamental common denominator for UC solutions; RTP is the additional denominator for all UC solutions other than text-based IM products. These standards, and the additional related protocols that enhance and strengthen additional service features (such as the ability to track quality of service, identify and allocate charges, etc.) are relied upon by those developing UC solutions to create the varied combinations of existing products and services within the field.

POTS and SIP Together

Step by step, UC products and services continue to compete, aggressively, against POTS, and the extensive physical infrastructure that supports POTS. Conventional telephones are replaced by VoIP devices; conference calls are scheduled and conducted through VoIP; IM is replacing conventional voice communication. But there remains, for the present time, a need to connect POTS and SIP services. Doing so allows POTS-initiated calls to be connected to SIP-enabled devices, as well as allowing SIP-enabled devices to route inbound calls to POTS telephone numbers.

Doing so is actually easier than might be imagined. UC providers have developed PBX devices that are capable of routing and managing both types of communications (these are often referred to as IPBX devices). IPBX devices are gaining acceptance and are appealing because they enable enterprises to configure the available services to their preferences. IPBX devices allow the appropriate controls to be established and enforced in order that internal calls may be routed through SIP protocols, while external communications can be routed through POTS services. In doing so, companies are able to benefit from the inherent security quality of the POTS infrastructure to protect their network content against unauthorized hacking or surveillance. But, as explored in Part II—Internet Security Services, many companies currently elect to prohibit inbound VoIP or other SIP-based content to cross their controlled network perimeters, in large part because of their reluctance to deploy IP-focused security controls and protective services against the inbound traffic.

Enterprise Management of UC Solutions—Key Decision Points

When a company elects to install one or more UC solutions, there are several decisions to be made that have consequences for the governance of the business, compliance execution and the management of legal risk. These decisions are particularly challenging because each involves (a) creating and managing different types of operating data that are necessary to assuring the quality and effectiveness of the services, and (b) influencing how the company will take steps to protect the integrity of its networks, computer systems, business records and personnel against improper content, hostile attacks or inappropriate use.

Companies usually consider the business case for any UC solution as a primary factor in purchase and implementation. Frequently, however, the answers to the following questions of legal risk and compliance are not considered by IT team members, to the potential detriment of the company and its business relationships:

What types of UC services will be allowed?

Selecting the UC services to be allowed, by necessity, requires the SIP servers to be configured and programmed consistent with the selections. Configuration and programming will enforce company determinations, such as:

- the types of SIP sessions that will be initiated.
- the types of RTP content that will be allowed to be received.
- the ports authorized to be used for approved SIP communications.
- the source locations, such as SIP addresses, that will be prohibited from establishing a session.[13]

What UC session-related content and data will be stored?

UC sessions generate different classes of content and data, nearly all of which can be stored and relied upon for legitimate business purposes. For example, a company can retain:

- Session logs, detailing the SIP data and, if applicable, RTP (or SRTP) data generated in connection with the session (addresses, date, time, duration, volume of data transmitted). Session logs are similar in their recorded data to the metadata associated with electronic mail records.[14] Session logs can also document:
  - Authentication and non-repudiation of session activity and content.
  - Enrollment and activity of multiple participants.
  - Note: Session logs are often necessary for tracking usage for internal and external billing purposes, verifying authorized use, and documenting the occurrence of specific events.
- Session content records, such as:
  - Instant messaging—text transcripts, attachments, web links, file transfers.
  - VoIP—conversation recordings (of the received digital packets, as well as converted audible analog versions).

[13] Internet security services routinely maintain lists of IP addresses associated with malicious or suspicious actors, ranging from credit card fraud, generators of spam mail and other malicious conduct.
[14] *See* RFC 3261-SIP: Session Initiation Protocol, available at http://tools.ietf.org/html/rfc3261.

- Video (including related audio)—recordings of the session, including additional interactive application sharing, chat or other content included in the session.

- Source records, such as:

  - original voice mail recordings that are converted to text messages.

  - text messages that are converted to audio recordings.

What uses will be made of any stored UC-related content or management data?

In the current regulatory climate emphasizing the sometimes conflicting policy agendas of privacy and security vs. transparency and availability, decisions regarding how stored content will be accessed or used can have important legal consequences. Obviously, any decisions on access and use should be documented, include a cross-disciplinary team (IT, legal and management) and, to the extent possible, implemented and enforced through appropriate controls.

Once involved, legal counsel needs to appreciate that, without regard to what may actually be said in a recording, stored UC content and management data is often indispensable to the ongoing delivery of the UC services and, as well, the protection of the networks, devices and property assets of a company, its employees, suppliers and customers. For example, here are examples of legitimate, necessary uses of stored content and management data that take no account of the actual words said by any participant:

- verifying the correct routing of SIP sessions through authorized ports and firewall services.

- collecting and validating log data required to calculate and allocate usage charges (for example, allocating the costs of UC services proportionately to actual usage among different departments), as well as to verify charges assessed by others (such as third-party service providers).

- auditing and evaluating the conversion quality of transferring content between formats to verify system accuracy, difficult words requiring editing within the conversion software, etc.

- auditing stored audio content in order to perform quality of service tests (evaluating gaps, garbles, silent patches and similar disruptions, for which adjustments can be made in the related software).

- the use of particular UC solutions (such as IM) to transmit links, attachments or other content in violation of corporate procedures limiting such usage.

Of course, companies must also consider whether:

- affirmative legal requirements impose an obligation to store UC content. For example, the United States Securities & Exchange Commission considers IM sessions with brokerage

customers to be subject to formal requirements to store and preserve those communications.[15]

- other duties exist to manage and preserve UC content or data as a result of other legal or business requirements, such as contractual obligations or complying with the scope of preservation orders affecting electronically stored information (ESI) in pending litigation.[16]

For all of the preceding, counsel's early and consistent involvement also helps assure that the legal implications of the many different configuration, storage and usage decisions are properly documented, taking account of the legal profile of the company, pending compliance and litigation duties, and ongoing business requirements.

Buy or Build

UC products and services present to enterprises the option of (a) acquiring and operating the core technologies and applications directly, or (b) contracting for the services to be delivered by a third-party service provider. Many third-party service providers also offer "public" versions of their products, as well as premium, private licensed versions that companies can acquire for internal support.

Instant messaging and VoIP have matured most quickly in this respect:

- Instant messaging management services include:
  - creating and managing archives of IM transcripts.
  - applying policy controls to monitor and regulate IM traffic, including attachments, and participants.
  - detecting and blocking inbound IM traffic containing malicious code, unauthorized content (such as SPIM—spam messages through IM; *see* Part II—Internet Security Services) and known suspicious IP addresses.
- Online conferencing services (such as WebEx or Adobe Connect Pro) integrate:
  - VoIP (as well as integrated use of POTS) for conference calls, programs and presentations.
  - IM/Chat sessions.
  - Live video sharing.

---

[15] 17 CFR 240.17a-4.

[16] The preservation of ESI in litigation has been especially controversial since Congress approved in 2006 amendments to the Federal Rules of Civil Procedure that specifically affirmed that ESI must be preserved and made available in civil discovery. http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. State rules, as well as similar rules in other countries, have been revised to reflect the federal changes. *See* www.ediscoverylaw.com for a complete list of those jurisdictions and links to the revised rules.

- Desktop or application sharing.

- VoIP public service providers (such as Skype or Vonage) integrate:
  - Voice communications (as well as integrated use of POTS).
  - IM/Chat sessions.

Internet architectural features generally allow virtually any UC solution to be delivered from outside an enterprise's firewall. Of course, doing so can have important implications for how a company addresses other management needs involving their UC-focused operations, such as governance, security risk management, risk allocation, business continuity and quality of service. These issues are common to any outsourcing services arrangement and UC solutions are no different in requiring the topics to be considered, particularly in negotiating, drafting and executing the related commercial agreements and service level agreements.

Generally, those agreements will include language that specifies the service provider to be an independent contractor (and, therefore, not considered part of the customer's legal entity). Whether an external UC solutions provider is independent or, for certain purposes, is considered an agent of the customer can have an impact on how the responsibilities of providing security and record keeping services are allocated and, in turn, how specific duties relevant to the legal compliance issues are performed.[17]

Protection of Property, Intellectual Property and the Rights of the Company and Others

Counsel has a further responsibility to assure that UC solutions (indeed, any IT solution), when implemented, do not place the property, assets and resources of their company at unacceptable risk. The business value of any UC solution can be dramatically undercut by a single adverse incident in which internal or external actors successfully exploit the UC solutions to expose a company's properties, assets and resources to disruption, loss or adverse legal consequences.

To be successful with this aspect of managing legal risk, counsel needs to appreciate the information security controls and practices used in connection with Internet services and the extent to which those controls and security practices are available to be used in connection with UC solutions. While it is likely not necessary for counsel to fully understand these technologies, it is useful to helping better align corporate policies and procedures (which *are* often under counsel's responsibilities) to avoid conflicts or gaps between those governance documents and the actual security services performed.

To do the job properly, counsel, working with IT and security team members, should:

- Create an asset inventory of the networks, systems, devices, applications and data that will be connected to and supported by the UC solutions and services.

[17] *See* Part IV—The Legal Analysis and Part V—Practice Toolkit for additional discussions of how to address this agency concept in implementing UC solutions.

- The objective is to document the properties and assets that require protection through the use of security services, and identify for those properties and assets the legal rights of the relevant parties in those assets.

- Many legal counsel are still learning how intellectual property rights (such as copyright, and confidentiality) attach to digital information. This exercise has the added benefit of advancing the maturity of those lawyers responsible for these properties.

- Produce a risk map, aligning the potential risks to which those properties are exposed, with the Internet security services that will be provided to protect those risks.

  - The objective is to document that those services are directly associated with protecting the property and assets of the company, the service providers employed (if different than the company) and the users (including the employees and contractors for the company that are the beneficial end users of the UC solutions).

As analyzed in Part III and Part IV of this Report, the preceding inventory and alignment activities are important to creating a synergy and interdependence between the risks that any Internet activities, including UC communications, present and the importance of the performance of the Internet security services to protect the rights and properties involved. These tasks are also incorporated into more complete checklists included in Part V.

Part II
Internet Security Services

Table of Contents

The Internet is now one of the world's fundamental technologies. Within a remarkably short blink in human history, we have engineered and continue to expand a communications network that makes the world accessible. The Internet delivers unprecedented access to information, accelerates business processes, transforms the efficiency of supply chains, financial services, business governance and is, a practical matter, a required resource for any company in business. But the Internet is also a significant avenue for those with malicious intentions. Through the Internet, bad actors target corporate networks and devices, seeking to acquire data with resale value in the black market, disrupt operations or otherwise exploit the vast information and service capabilities to which they may gain access.

While unified communications offer a compelling business case, the strength of UC solutions in leveraging the Internet to transform how we communicate is also a vulnerability. Not only are UC solutions exposed to security vulnerabilities and risks that the Internet presents for other corporate network activity, but the availability (and relative youth) of UC solutions has encouraged malicious actors to develop and launch new types of attacks and hostile activities that specifically target UC solutions. The identities of these actors continue to evolve, but public discussions, government publications and conferences have confirmed organized crime syndicates, nation states, fraud and scam artists, and curious, technically inclined teenagers are all among those waging attacks against corporate systems, property and data.

This Part II serves to (a) identify the types of security risks and vulnerabilities against which corporate information security services are directed, both for Internet services generally and specific UC solutions, and (b) describe the types of security services that can be integrated into how UC solutions are delivered, in order to protect against the related risks and vulnerabilities. Internet security services work, individually and collectively, toward several key business objectives:

- Protecting the facilities, equipment and properties (both technology and data) of the company.
- Protecting the rights of the company and the users with respect to the facilities, equipment and properties (including the intellectual property rights in the data and information).
- Protecting other providers with whom a company connects in the overall networked community of those moving communications to and from the company.

Note: Internet security services, and the types of exploits and vulnerabilities involved, are extremely complex and technologically sophisticated. This Part II is intentionally oriented toward the perspective of a corporate lawyer that has limited technology training or experience with information security. As a result, the level of detail and overall scope may be viewed by security professionals as under-inclusive.

This Part II should be considered as a starting point for dialogue between counsel and other members of the corporate team implementing UC solutions, and is not a replacement for the value a qualified information security professional can contribute by identifying more completely the threat profile a specific company may face, the security controls that are employed and how those matters are affected by the specific UC solutions a company is implementing.

As with any corporate program, the success of Internet security services can be heavily influenced by budgeting, staff capability, availability of responsive technologies and defenses, effectiveness of internal training, and changing external requirements (from vendors, customers, and regulatory authorities).

Types of Security Risks

Bad actors targeting corporate networks, devices and data will consider themselves successful if they only achieve their objectives once out of several hundred attacks. As a result, many of the types of conduct that present security risks will often be scaled at levels that are shocking in volume and intensity to those unfamiliar with the circumstances. "Brute force" attacks, for example, use exhaustive trial and error methods for identifying passwords, log-in identification codes and other valuable keys of access that can generate tens of thousands of attempts on a daily basis.

The following terms are useful in discussing information security; these are relied on later in offering lists of both general Internet security risks and those unique to UC solutions and services.

Term	Meaning
Threats	Threats or threat sources are the actors or situations that are the originating source of a possible security incident
Vulnerability	A flaw or weakness in a system's procedures, design, implementation or controls that can be exploited, resulting in a security incident
Impacts	The adverse impacts, consequences or outcomes resulting from security incidents
Risks	The result of threats acting against vulnerabilities to cause impacts
Incident	A specific activity or action for which a security risk occurrence is probable; incidents trigger investigations and responses, but may not result in actual disruption or loss
Controls	The controls or countermeasures deployed to reduce or constrain threats, vulnerabilities or impacts

Information security, in its essence, involves aligning controls as effective defenses and countermeasures against potential risks. Many of the controls implemented by information security are

automated and configured to operate in real-time as data approaches across the Internet and seeks entry onto the corporate network (the perimeter of a network is often established by a "firewall", one or more computer servers that control the transport of data into and out of a corporate network). The firewall, and the corresponding controls, rely heavily on the packet header information on inbound packets to properly evaluate, route and potentially reject inbound data.

The introduction of any new component or service within a company's computing services portfolio challenges information security to adapt and respond. Bad actors exploit that reality, and can be successful at figuring out vulnerabilities that can be attacked, and conducting successful attacks, before the new product vendors and their customers can recognize the vulnerabilities and develop appropriate defenses. The time periods in which these attack and defense maneuvers occur are dramatic—security professionals refer to "zero-day" attacks, which are those in which the attack vector has been exploited and distributed within the bad actor networks before either the public, product vendors or their customers are aware of the existence of the attack, much less able to release and install the patches or other controls required to defeat the new attack methods.

Bad actors are so diverse in their motives, methods and means that any structural definition of the security risks connected with the Internet will be under-inclusive. Bad actors can and do target the full range of properties and assets of a company, but often with very focused and narrow objectives. Virtually any connection to the Internet or any communication activity or data asset can be exploited to attack a corporate network or device.

Like attacking a castle, once the perimeter of a corporate system has been breached, the bad actors (or their software agents) act to further compromise the system, acquire data assets, establish and exploit unauthorized access to services, and disrupt operational command and control. Achieving effective security requires continued vigilance and investment, and the absence of that discipline will magnify the potential damages that can result from any successful attack.

Against these types of risks, the information security profession develops responses. While many of the responses, as controls, are reactive to new threats, there is increased awareness that improved discipline in how software programs are developed from inception can affect the level of security risks that any new component or service may present. "Software assurance" incorporates into the application development process a focus on known security risks and, in turn, implements controls in the related software code in order to better protect an application against security risks. Software assurance also involves scanning software code in order to detect potential malicious code files; as developers increasingly rely on open source code to assemble applications, this latter aspect of software assurance is especially important.

Security Challenges in Unified Communications

Telecommunications networks have been traditionally modeled as a series of "planes," separating traffic content into three distinct classifications:

- The management plane is responsible for the management of all elements in the network.

- The signaling plane is responsible for the control, support, and establishment of the media (or bearer) plane.
- The media (or bearer) plane is responsible for the transport of the actual network content payload.

This model is equally applicable for commercial carrier networks as well as enterprise telecommunications networks.

In traditional telephony (i.e., POTS), these planes are actually operated as physically separate and distinct networks. However, with UC solutions, the different networks use a common IP network infrastructure for all network traffic, whether it is management traffic, network signaling/control traffic or end-user voice or multimedia traffic. The three "planes" have been collapsed into one physical network, namely the IP network infrastructure of the Internet. As a result, an array of known Internet threats now also become potential threats to the new communications service infrastructure and the content carried across it.

What types of risks are targeted by information security at the firewall of a corporate network? The next table lists significant threats, the vulnerabilities they target and the potential impacts common to corporate networks connected to the Internet, but this is not a list of all risks against which information security programs are directed. Since UC solutions are Internet-based, all of these risks challenge any UC solutions or services just as they confront any other Internet-based communication services:

Threat	Vulnerability	Impact
Loss of Confidentiality	Internet traffic, by itself (i.e., without security services), has no inherent mechanism for data confidentiality.	• Unauthorized people or entities can easily observe data. Both privacy and confidentiality can be compromised. • Bearer, signaling and management traffic can be intercepted. • Unauthorized interception of critical data such as voice or multimedia communications, passwords or credit card numbers is possible. • Analysis of what addresses (phone numbers called) are accessed and when can be obtained. • Network attackers could potentially eavesdrop on sensitive signaling information • Trojan horse programs could be installed in end user devices or network equipment, which could potentially be used to enable eavesdropping.
Loss of Integrity	Internet traffic, by itself, has no inherent data integrity protection.	• Unauthorized manipulation of critical network data or equipment configurations could cause service disruptions. • Could be used to allow theft of service and tool fraud. • Malware such as viruses, worms and Trojan horse

		programs may compromise the integrity of network equipment.
Loss of Availability	Internet traffic, by itself, has no inherent availability protection mechanisms; quality of service controls are present by not widely used.	• Denial-of-Service and Distributed-Denial-of- Service Attacks can be used to source flooding attacks which flood network devices with excessive data. • Malformed packet attacks can be initiated by modifying packet formats, and headers may be purposely injected into the network to cause equipment failures and resets. • Network attackers could cause network disruptions or denial of service conditions by mis-configuring or resetting network equipment .

Specific UC Security Risks

During the short, energetic life of UC solutions in the market, bad actors have moved rapidly to develop attacks and tools that exploit the solutions in order to acquire valuable corporate data or make unauthorized use of the corporate networks or facilities. Here are some representative security risks associated with unified communications:

Malware—Hostile applications (crimeware, rootkits, exploits and other malware) can be disguised inside a variety of inbound packet payloads. Malware can also be carried in attachments or links communicated through IM, e-mail or other message tools.[1] Malware can include: viruses, spyware, bot-nets (converting individual devices into spam mail servers), etc.

Trojan Horse—Hostile applications that are installed in end user devices or network equipment, which can potentially be used to enable eavesdropping, or execute specific programs based on certain events, times or circumstances.

Code Injection—a specific type of malware in which the injected code succeeds in altering the normal performance of a computer device. For UC services, for example, code injection could cause substantive payload content to be intercepted and re-directed to a device external to the corporate network.

SPIM (Spam over Instant Messaging)—Public IM services allow members to send unsolicited session requests to others (much like unsolicited e-mail). SPIM has the same type of adverse impact on operations as e-mail spam: service degradation, storage capacity, malware transport, diversion of human resources, etc.

[1] One commercial website publishes a list of currently known malware that targets IM, listing over 40 different known exploits. *See* Instant Messaging Security Center at http://www.quest.com/im-security-center (last visited April 10, 2009).

SPIT (Spam over Internet Telephony)—Unsolicited telephone calls over IP networks into a corporate network can be originated from known hostile servers, as well as servers that have been compromised (without the knowledge of the server owner).

Phone Fraud—Acquiring unauthorized access to VoIP capabilities in order to conduct unauthorized telephone communications (without charge). This can be accomplished, among other means, by credential harvesting, a technique of tricking VoIP devices to transmit authentication credentials required to access a company's network.

Intercepted Communications—Previously successful malware installations can locate and intercept communications without notice to any participant. Interceptions can also occur at gateways or connected servers through which communications are being routed. Of course, these types of interceptions are illegal under ECPA, but enforcement is difficult given the challenges of identifying the intercept and acquiring jurisdiction over the malicious actors.

War Dialing—a coordinated calling attack that attempts to identify an insecure modem or device that can be used as an access point into a corporate network. Dialing strategies are built around a single known number.

Fuzzing—the inbound packets are overloaded with content, including in the header (such as an extra long inbound IP address; resulting processing failures may expose vulnerabilities that can be exploited.

Effective Security Controls

When recognized Internet-based security threats are enhanced by the new threats directed at UC solutions, the risks to the property and rights of the corporation offering those solutions to their employees and business network can be substantial. In response, there are a number of security controls to be employed.

The following list highlights the type of controls and, with a focus on how UC services work (see Part I—Understanding Unified Communications), the manner in which those controls interact with how SIP sessions and IP packets are created, transported and processed. *None* of these controls require the provider of the UC service to "listen" to any audible version of any oral conversation that may be part of a SIP session; the security analyses and controls are purely applied at a packet level.

IP Address of Inbound Packets—Firewalls and attached devices will identify and evaluate the IP address (e.g., set forth in the header for a general IP data packet) in order to:

- validate the address against a list of known, approved addresses.
- compare the address against a list of known disapproved or malicious addresses.
- re-direct any suspicious address into a quarantined location for additional analysis.

Note: the scans required for this service do not require, or access, any payload content of the packets.

SIP and RTP/SRTP Address and Transaction Data—Similarly, the same type of scans are conducted with respect to the additional transaction data arising from SIP-based communication sessions and messages.

Content Tags on Inbound Packets—Within the headers of SIP-based packets, additional identifier information will designate the content type within the packet payload (IM, voice, video, audio). Similarly, attachments or links are readily recognized (many policies prohibit the communication of attachments or links through services, such as UC, for which the filter controls used on e-mail are not available). Prohibited content types can be recognized and the packets rejected or diverted into a quarantined location.

Payload Consistency—Security controls will compare the content tags to the payload attributes; if there are inconsistencies in the formatting (e.g., software code appearing in a packet labeled as voice), the packets will be rejected or diverted.

Payload Integrity—Antivirus programs analyze payload content to identify the "virus signature" of hostile or malicious code. Packets will be rejected or diverted if "virus signatures" are recognized.

Session Log Analysis—Session logs of completed SIP sessions can be analyzed to evaluate that the SIP session was properly configured and that only authorized message formats and content types were processed. For this purpose, the analysis focuses on data elements such as the ports used, IP/SIP/RTP data, and related routing and management data. Activities inconsistent with usage permissions, recognized usage patterns or other metrics for consistent operations can be the basis for further forensic investigation.

Forwarding Instructions/Log Analysis—UC services may allow users to forward, prioritize or route communications, including to remote or mobile devices. Security controls can limit the acceptance of those instructions to approved parameters, and/or may review transaction logs to confirm no instructions were provided to direct or forward communications outside the controlled perimeter of approved devices (e.g., to an insecure home computer).

Encryption—Contemplated by the SRTP protocol, the use of encryption among communication participants can protect the devices and frustrate the attempts of malicious actors to intercept or divert communication content or transaction data.

The preceding examples emphasize that effective security services can be, and are, applied to UC services without putting at risk any expectations any user may have regarding the exposure of their communications to interception or undisclosed real-time access.

Additional Security Considerations

While Internet security services emphasize defending the perimeter, effective security also focuses on many other aspects of a company's operations. Those services also extend logically to any contemplated use of UC solutions. Since VoIP/multimedia traffic have specific real-time characteristics that require proper processing to avoid network delay and jitter, security solutions can challenges. The solutions must preserve the real time characteristics of VoIP/Multimedia traffic and not add significantly to network processing overheads. In addition, voice and real time services must be available when required, and security mechanisms cannot delay the delivery of services.

Here is a list of some security services that may be applied:

- Software code integrity—Any new software application or device on which software is installed should be tested to confirm the code itself has integrity and both lacks known malicious code, as well as known vulnerabilities that can be exploited.

- Internal audits of configuration logs—In addition to user log analysis, additional audits of configuration logs may also identify configuration changes that were installed from external malware or other bad actors. SCAP services, such as those on which the Internet Security Alliance is contributing toward their development (*see* Introduction), accelerate configuration log review toward real-time analysis and corrective actions. One example might be a configuration that overrides existing settings in order that IM session content may be stored for later malicious export, a change normal users may not detect.

- Content usage logs—Content delivered through UC sessions can legitimately be stored (for example, the conversations held with security brokerage customers pursuant to SEC rules). However, usage log analysis may detect any improper attempts or successful unauthorized access to the content, without accessing the content itself.

- Vendor enterprise security—If some or all of the UC services are being delivered by a third party service provider, customers will often require that the facilities and systems of the vendors be managed effectively for information security purposes. Vendor security can be tested and stressed by a variety of security attacks, all designed to measure and validate the effectiveness of installed controls.

Managing Information Security

Information security, to be effective, must be performed with the discipline of any well-managed program. This necessity is beginning to influence regulatory agencies in how they view the importance of information security to assuring the trust that is required in the businesses subject to their jurisdiction. Independent of the legal requirements surveyed in Part III-The Legal Landscape, there is continuing momentum toward viewing information security as a corporate program for which a

management system is appropriate. At the national and state level, increasingly explicit requirements are being enacted.[2]

The International Standards Organization publishes a portfolio of standards that define the elements for an information security management system (ISMS) and the programmatic elements needed for supporting ongoing responses to shifting threats, vulnerabilities and risks.[3] Those standards emphasize three components that benefit greatly from the input and awareness of legal counsel:

- Policies and procedures for the information security program should be developed and maintained as records pursuant to the corporation's records management services. For any communication services, including UC solutions and services, policies should address specifically the ownership and access rights of the company and its agents, as well as the expectations of users for potential monitoring of their communications. There are many commercial resources providing guidance on how to develop these policies and Part V—Practice Toolkit highlights additional details to be considered.

- Program documentation should be developed and maintained that tracks ongoing performance of the security services. From a compliance perspective, this documentation can serve multiple purposes:

    - Capture performance data that allows ongoing program services to be evaluated against their criteria.

    - Demonstrate the consistency of use for the varied stored information assets (such as transaction data as well as primary or source communication files).

    - Generate data that evidences compliance with applicable explicit legal requirements.

- Employing performance data and metrics to communicate to management the overall effectiveness of security services and the steps required, in a program of continuous improvement, to adapt security services to new threats, vulnerabilities and risks. Since the types of reports generated in this regard may have evidential significance, counsel's awareness of their contents is recommended.

[2] Many of these are discussed in further detail in Part III of this Report and in resources listed in Appendix 2—Legal and IT Resource Inventory.

[3] These standards are generally organized as part of the 27000 series of published ISO standards, notably ISO/IEC 27001:2005, Information technology—Security techniques—Information security management systems—Requirements. Information on purchasing these and other ISO standards is included in Appendix 2—Legal and IT Resource Inventory.

Part III
The Legal Landscape

Table of Contents

1. Introduction

Electronic communications in the 21st century proceed forward within a legal infrastructure that is struggling to keep up with the pace of change. New technical challenges in information processing, computing, network services and storage activities, as well as the criminal and civil misconduct that exist, make bridging this gap a growing priority for legislators and industry participants alike. Key principles of ownership, control, property rights and governmental authority that have informed how corporations define and manage legal risk are increasingly strained by the impact of computing and digital information.

Lawmakers are trying to respond effectively, but many of the law reforms for electronic commercial practices, and the ensuing malicious misconduct, are often reactive and outpaced by changes in technology that were not contemplated in the enactment process. Regulators have sought to be more responsive, sometimes straining the scope of their jurisdiction in order to remain relevant and effective

in light of changing technologies. Lawyers are also struggling, since effective counsel for their clients requires them to learn and understand both new information technologies and the changing legal landscape.

Those deploying unified communication solutions face a legal framework that reflects all of these characteristics—reactive lawmaking, laws strained by changing technology, aggressive regulators, and lawyers (and their clients) left with unanswered questions that have handicapped their enthusiasm for adopting new technologies. Indeed, the genesis for this Report were very real concerns among senior IT professionals and lawyers that the use of conventional Internet security services to protect the property and rights of a company deploying UC services would be illegal or expose the company to unacceptable legal risks under 20th century laws enacted before the Internet achieved commercial viability.

This Part III examines the existing laws that significantly frame the current legal environment for unified communications.

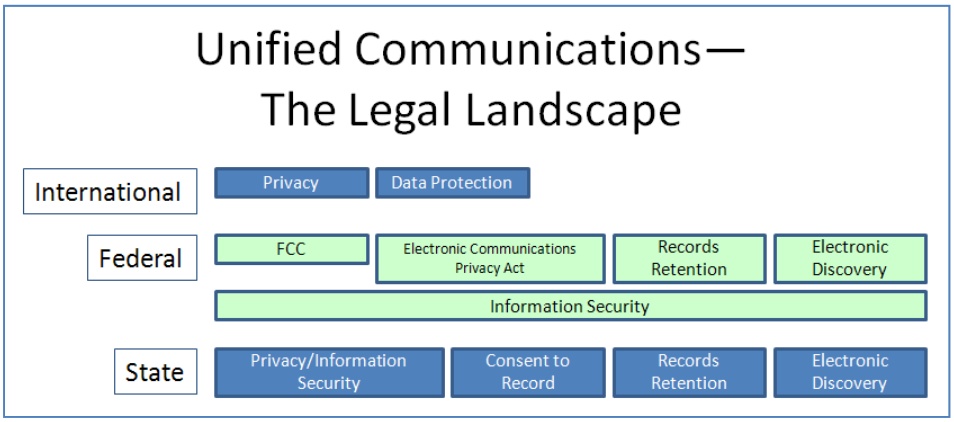
- Section 2 of this Part III surveys the relevant laws, focusing on US federal laws, but also giving attention to selected state laws and international privacy requirements. The analysis emphasizes that, among all of those laws, only one—the Electronic Communications Privacy Act (ECPA)—requires detailed consideration.

  For the rest of the laws, whether or not a company uses more traditional communication technologies or deploys UC solutions has little impact on the duties of the company as a provider of the UC solutions. Part V—Practice Toolkit includes references to these other compliance topics in the checklists that are included.

- Section 3 reviews the ECPA provisions in detail, the state laws requiring consent to the recording of telephone conversations and the implications of those laws for UC solutions and services.

- Section 4 analyzes in further detail the defined terms under ECPA and describes those activities which ECPA expressly provides are not unlawful. The discussion highlights, for UC solutions teams (technologists, security officers and lawyers), the questions we considered in aligning ECPA to UC services, which questions are then answered in Part IV—The Legal Analysis.

2. Relevant Laws and Regulations



The global, boundary-crossing quality of the Internet challenges any company to determine which laws may actually apply to any specific activities they conduct. Traditional legal principles of how nations or individual states enforce their laws outside the physical boundaries of their jurisdictions are also evolving, particularly as political entities act to protect their citizens and businesses against malicious actors on a global scale. As a result, a full inventory of all of the potential rules to be navigated in achieving compliance for unified communications is beyond the scope of this Report. Instead, we have focused on the following, which accounts for the key laws any company conducting business in the United States should prioritize in evaluating UC solutions.

2.1 Federal Communications Commission Orders

Under the Communications Act of 1934, as amended, the Federal Communications Commission (FCC) has traditionally exercised their authority on "telecommunication carriers"[1]. The Internet has challenged the FCC to think differently, however, on the boundaries of their enforcement authority. Until the last five years, the FCC had concluded the services required to alter the format of information through computer processing applications justified Internet service providers being separately classified as "information services."[2]

Under the authority of the Communications Assistance for Law Enforcement Act in 1994 ("CALEA"), the FCC was asked by the Department of Justice to evaluate how those providing VoIP services were to be

[1] "The definition of 'telecommunications carrier' includes such service providers as local exchange carriers, interexchange carriers, competitive access providers, cellular carriers, providers of personal communications services, satellite- based service providers, cable operators, and electric and other utilities that provide telecommunications services for hire to the public, and any other wireline or wireless service for hire to the public." , 15 FCC Rcd. 7105 (2000) (*Second Report and Order*) at 7111, para. 10 (citing 140 Cong. Rec. H-10779 (daily ed. Oct. 7, 1994) (statement of Rep. Hyde)); *see also* H.R. Rep. No. 103-827(I), at 23, reprinted in 1994 U.S.C.C.A.N. 3489, 3500 (*House Report*). The critical FCC orders reviewed in this analysis are listed in Appendix 2—Legal and IT Resource Inventory.

[2] Report to Congress, 13 FCC Rcd at 11516-17, para. 33 (quoting Federal-State Joint Board on Universal Service, CC Docket No. 96-45, Report and Order, 12 FCC Rcd 8776, 9179-80, paras. 788-89 (1997)). *See, contra,* United States Telecom Ass'n v. FCC, 227 F.3d 450, 464-66 (D.C. Cir. 2000) (applying telecommunication rules to certain packet-switching services).

classified under the Communications Act.[3] At issue was the jurisdiction of the FCC to require that "telecommunications carriers" comply with federal standards that required communication technologies be designed in order to enable allow lawful interceptions of voice communications by law enforcement authorities, and obligated the service providers to be accessible to law enforcement for those purposes.

In 2005, the FCC reached two meaningful conclusions:

> First: "In today's technological environment, where IP-based broadband networks are rapidly replacing the legacy narrowband circuit-switched network, various types of packet-mode equipment are increasingly being deployed to "originate, terminate, or direct communications" to their intended destinations".[4]
>
> Second: Based on the "substantial replacement provision" in the Communications Act, the FCC concluded VoIP services were substantially replacing traditional wireline services (POTS) and, as a result, Congress intended to preserve the availability of the related switching and routing technologies to permit lawful intercept activities by law enforcement authorities.[5]

This determination had the effect of classifying as "telecommunication service providers" those acting as operators of interconnected VoIP services under CALEA, even if they were not so classified under the Communications Act.

The FCC has since taken two additional actions which assert further requirements on the equipment used for VoIP services:

- The equipment must support access for disabled individuals.[6]
- The equipment must support emergency call capabilities (9-1-1).[7]

None of these FCC Orders present compliance challenges to the ordinary operation of the technologies used for UC solutions and services. However, any company directly acquiring those technologies or contracting for the services from other providers should take the steps necessary to assure their technologies comply with FCC requirements (items addressing those steps are included in the checklists included in Part V—Practice Toolkit).

Some enterprises have elected, in light of the FCC orders, to not acquire VoIP technologies in order to avoid the related requirements of potential cooperation with law enforcement. That is entirely a

---

[3] FCC 05-153, First Report and Order and Further Notice of Proposed Rulemaking, Adopted: August 5, 2005 Released: September 23, 2005. 20 FCC Rcd. 14989 (Sept. 23, 2005) (hereinafter "First Report").
[4] First Report at p. 6.
[5] Id.
[6] 22 FCC Rcd. 11275, ¶ 21 (2007).
[7] E911 Requirements for IP-Enabled Service Providers, No. 04-36, Comments of Dialpad Communications, Inc. *et al.,* at 4; Comments of Level 3 Communications at 13- 14 (filed May 28, 2004).

business decision, but that course of action does not avoid the intercept powers of the federal government. In the absence of VoIP, the POTS switches carrying wireline circuits to the company remain accessible for warranted intercepts sponsored by law enforcement. Realistically, all that a decision against VoIP avoids are the added costs of supporting disability access and emergency call capabilities.

One factor that cannot be entirely anticipated in the near-term future is the degree to which the FCC, the Department of Justice, the Department of Homeland Security and other federal stakeholders will reconcile, restate or otherwise improve the consistency with which Internet-based services are subject to regulation. UC solutions customers should remain watchful for further developments in this area.[8]

2.2 State Privacy and Data Security Laws

Provoked by consumer concerns regarding the privacy of personal information held by online retailers, financial service providers, health care providers and others, numerous states have enacted laws that establish requirements affecting the protections personal information records are to be afforded and, in turn, the corporate information security services required to do so. These laws complement federal laws addressing personal information in selected industries; collectively, they functionally extend consistent privacy protection to citizens in the absence of more comprehensive federal legislation.[9]

For companies deploying UC solutions, whether in or outside of industries touched by existing federal law, the state privacy laws may require specific information security controls to be implemented to protect personal information collected or created as part of the UC services (e.g., communication transaction data and usage records, as well as substantive content—the content of e-mails and IM—that is protected as personal information).

These state privacy laws share an aggressive approach to the authority of the state or any citizen to enforce the laws; generally, the laws apply to any person conducting business in a state or owning, licensing or maintaining personal information about a resident, regardless of their location.[10] For most consumer-facing businesses, these laws have a practical effect of driving companies to find a common denominator in their business practices that will satisfy the legal standards of any state in which business is conducted or citizen personal information is maintained. However, there are significant variations in how the states address the use of information security in handling personal information

[8] The Internet Security Alliance participated actively in submitting comments to the Cybersecurity review conducted in early 2009 under the direction of Melissa Hathaway, acting senior director for cyberspace of the National Security Council (NSC) and the Homeland Security Council (HSC). *See, generally,* http://www.whitehouse.gov/the_press_office/advisorstoconductimmediatecybersecurityreview/. Comments submitted by the Internet Security Alliance included attention to the costs and inefficiencies faced by industry in attempting to monitor and comply with multiple regulatory frameworks touching upon Internet services and effective information security. *See* www.isalliance.org.

[9] See Section 3.2 for a discussion of those Federal rules. A detailed analysis of the state privacy laws can be found at http://epic.org/privacy/consumer/states.html (last visited May 17, 2009).

[10] Whether any company has the "requisite contacts" with a state to be held accountable under its laws, in the absence of physically being present in the state, has been the subject of an enormous number of cases during the last few decades. *See, e.g., Kearney v. Salomon Smith Barney*, 39 Cal.4th 95, 137 P.3d 914 (Cal. 2006).

which make that "common denominator" strategy more challenging. California and Massachusetts illustrate that challenge.

California

California enacted SB 1386 in 2003, and its enactment served as a model for other state enactments.[11] The California law was applicable to any entity conducting business in California, or owning or licensing "personal information" to notify the individuals affected when such entities know, or have reason to believe, the related personal information has been accessed without authorization.

Personal Information under California SB 1386

First name (or initial) and last name, combined with one or more of the following (when either the name or the data elements are not encrypted):

- Social security number.
- Driver's license number or California Identification Card number.
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

However, the notification duty only exists if the personal information that has been accessed was "not encrypted" (see sidebar language). Apparently, California concluded that a company employing encryption to protect personal information was exercising a "defensible" standard of care and should be excused from the notification duty. But, for those companies holding personal information, lawyers and technologists have struggled to determine what constitutes the appropriate use of encryption that assures non-liability, and there is no clear answer presently.

Massachusetts

The California law set in place the marker that states are willing to examine and define information security services as a basis for protecting the citizens' interests in their own information. In 2007, the Commonwealth of Massachusetts moved beyond the encryption requirements of California SB 1386 and enacted a security breach and data destruction law that has been described as "the most comprehensive set of general data security obligations yet to be imposed on businesses by a state".[12] The Massachusetts definition of "personal information" tracks the California scope, but requires the relevant data custodians to "develop, implement,

[11] CA SB 1386 (2003), available at http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

[12] Smedinghoff and Hamady, "New Data Security Regulations Create Compliance Challenges for Businesses," The Secure Times (Vol.4, No.1, 2009), at 2, available at http://privacylaw.wildman.com/article/Secure_Times_Winter_2009.pdf. (Last visited April 28, 2009).

maintain and monitor a comprehensive, written information security program."[13] In addition, mandatory encryption is required for personal information on stored on company laptops and portable devices, in files transmitted over public networks and when transmitted wirelessly. Additional regulations detail the elements for an effective information security program.[14] Compliance requirements have been extended until January 1, 2010.

For most companies, the election to deploy UC solutions is unlikely to alter whether or not they must comply with applicable state privacy laws. Given the precision of how "personal information" is defined, tilting toward consumer financial data and particularly sensitive non-medical consumer information, these laws have a broad impact, but their applicability is not based on whether a company is migrating from existing Internet-based services to UC services.

If existing services are being migrated, a company must simply extend their existing compliance process to also cover the transport and storage of the qualifying personal information through the new services. Similarly, if new services are being introduced, such as allowing IM with customers, companies need to develop suitable policies and instructions to address whether qualifying personal information will be transported or maintained in connection with that service. Part V—Practice Toolkit includes references to state privacy laws in the relevant checklists.

2.3 International Privacy Laws

During the last 25 years, a robust body of law has developed that establishes rules on the collection, storage and use of personal information. The laws, and their application, continue to evolve, with new technologies, and competing public policy interests (such as counter-terrorism) provoking adaptations and refinements in what is permitted and prohibited.

Outside of the United States, current national laws, particularly in Europe, reflect a significant commitment to privacy as a personal right, as opposed to a statutory right protecting specific classes of information (educational records, health records, financial data, etc.). This alternative approach has created significant challenges for companies conducting international business. One of the key principles of these laws is that the rights of the individual attach to data based on their residency, regardless of where data may be specifically collected or maintained.[15] Many jurisdictions have also enacted rules that limit the movement of personal data across national boundaries.[16]

These laws also include requirements that define different standards of protection (such as information security) to be afforded to different classes of personal information. Meeting those standards often

---

[13] 201 CMR 17.00 (2009), *Id.*
[14] *Id.*
[15] *See, generally,* http://epic.org/privacy/consumer/states.html.
[16] *See, generally,* Rotenberg, The Privacy Law Sourcebook (Electronic Privacy Information Center, 2004). An online resource is available at Data Protection and Privacy Law, http://www.privacylaws.com. Numerous other sources exist online for researching international privacy laws. An important resource for conducting business in the United States involving personal information of non-US citizens is the Safe Harbor program, available at http://www.export.gov/safeharbor/index.asp (last visited April 17, 2009).

involves, and is sometimes required to include, installing and operating different types of information security controls (including minimum guidelines on password length and management).[17]

Many services that UC solutions enable may offer new channels through which personal information can be collected, transmitted or received (such as IM). In addition, the solutions may enable different movements of information within the enterprise or among those to whom an enterprise may be connected. After all, UC solutions exist to improve collaboration and efficiency; overcoming distances and accessibility to controlled information are some of the advantages to be realized. As a result, care is required to assure that the proper corporate policies and procedures are in place.

For most companies implementing UC solutions, any impact of international privacy laws has already shaped their management of personal information, including the security, access and transfer controls required to assure compliance. However, for companies for whom the UC solutions may introduce new, more efficient means to transfer or access personal data, existing policies and controls need to be updated to extend their requirements. For those whom the UC solutions open entirely new methods, new policies are needed if the existing ones did not already properly address the types of activities and data protection features required for compliance. Part V—Practice Toolkit includes references to these action items in the related checklists and materials.

2.4 Requirements for Retaining Records and Information

Records and information management is rapidly maturing as an important service supporting corporate governance, regulatory compliance and the management of legal risks, including those arising in the courtroom. From the 20th century stereotype of a warehouse filled with dusty boxes, modern business practices are increasingly focused on capturing, storing and retaining the availability of business records and information. In a global environment in which more than 97% of all business information is originated digitally, the records and information management function is inherently required to be part of the overall agenda for IT governance and operations.

Recent headlines have emphasized that companies which neglect their records management functions, or perform them poorly, particularly in locating records required as potential evidence in the courtroom, can face catastrophic legal and business adversity. The sanctions and fines against poor records management can often be measured as millions (and even billions) of dollars.[18] Slowly, if only to avoid the risks of those sanctions being imposed directly against them, corporations are investing in records management services that integrate the compliance duties into how IT services are deployed. Nevertheless, for the records manager, one of the persistent continuing challenges is assuring that (a) new services are evaluated in order to understand how they impact existing policies and procedures for retaining specific classifications of records, and (b) the new services are aligned to any known legal requirements for records preservation and retention. Implementing UC solutions are no different—

[17] *See* sources noted in preceding two notes.

[18] *See, generally,* research and materials available at www.ediscoverylaw.com, www.sedonaconference.org, www.edrm.net, www.discoveryresources.org, and other commercial websites and published materials.

records management should be part of the enterprise team undertaking the process. Part V—Project Toolkit includes attention to records management topics in the checklists and materials included.

Records managers have responsibility for knowing the international, national, state and local requirements for retaining business records, and developing appropriate controls and processes for assuring compliance. However, recent shifts in the law that respond to the emergence of digital business practices and the use of Internet-based communications have generated several new threads in the records retention legal landscape that need to be considered in navigating compliance for UC solutions:

Electronic Communication Records—Various laws classify communications in which certain types of citizens participate as important records to be retained. Before the Internet, those records may have consisted (by example, for securities brokerage firms) solely of written orders, correspondence or confirmations, while today, the same communications can occur through Internet-based services, such as electronic mail. Regulators recognize that Internet-based services could potentially allow those they regulate to bypass their records management duties, and, in response the regulations have consistently been revised at all levels of government to expressly reference new communication formats. Health care and financial services are two additional industries where similar regulatory reforms continue to adapt in order to better reference digital communications.[19]

Those implementing UC solutions cannot overlook the existence of these requirements; to the extent the UC solutions being deployed introduce new communication formats (such as IM with external customers), the compliance agenda needs to include appropriate attention to assuring that the communication records are properly identified, classified and preserved within the records management program.

European Data Retention Rules

In 2006, responding to calls for more effective investigation capabilities regarding international terrorism, the European Parliament enacted a controversial Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.[20] Pursuant to this Directive, internet service providers and others providing publicly available services must capture and retain any data relating to telephone or Internet communications (enumerating specifically over 30 different data types to be retained), *other than the actual content of the communications*

[19] The 2009 Stimulus Bill, enacted as Public Law No. 111-5, included specific provisions on information security for health records. Available at http://thomas.loc.gov/cgi-bin/bdquery/z?d111:h.r.00001. *See, generally,* "Stimulus bill includes protection for digital health care records", at http://www.scmagazineus.com/Stimulus-bill-includes-protection-for-digital-health-care-records/article/126694/.

[20] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML (last visited April 20, 2009) ("2006 Directive").

itself.[21] Pursuant to the Directive, member states in the European Union must adopt enabling legislation and regulations.[22]

Similar to the definitional challenges under the U.S. Communications Act (discussed in Section 2.1 above), European countries may need to resolve which entities are recognized as public electronic communication services to which the 2006 Directive (and enabling national laws) will apply. For example, under the laws of the United Kingdom, a public electronic communications network is "an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public."[23] However, it is currently unclear whether, for example, an IM/Chat/VoIP capability integrated into a retailer's website, allowing potential customers in the public to communicate with the retailer's shopping staff, will be classified as a public electronic communications network or service.

Under United States law (as discussed in Section 3 below), the types of data to be collected and retained under the 2006 Directive are considered as transactions data and, in marked contrast to the European Directive, not subject to specific retention rules. Moreover, under US law, there appears to be no precedent on which to conclude that a privately operated UC solution or service, such as that just described in the preceding paragraph, would be viewed as a service being offered to the public.

Those deploying UC solutions should evaluate whether the scope and nature of their operations of those solutions requires any transactions data (or its equivalent) to be captured and preserved by the laws relevant to the jurisdictions in which the services are operated.

Electronic Discovery Obligations to Preserve Potential Evidence

In December, 2006, the Federal Rules of Civil Procedure in the United States were amended to confirm and clarify the legal duties of those in civil lawsuits to preserve and produce potential evidence that may be electronically stored information ("ESI").[24] Many of the states have now adopted similar laws, and other nations have proceeded in the same direction.[25]

Across this portfolio of "new" rules, there are no limiting definitions of the types of ESI that may be required to be identified, collected and preserved for possible future production. Indeed, many case decisions have affirmed that a party's duties can extend to any type of reasonably

---

[21] 2006 Directive, Article 5.
[22] The United Kingdom regulations are 2007 No. 2199, available at http://www.opsi.gov.uk/si/si2007/uksi_20072199_en_1 (last visited April 20, 2009).
[23] Id. at Section 2(e). Communications Act at Section 151(1), available at http://www.opsi.gov.uk/acts/acts2003/ukpga_20030021_en_15#pt2-ch1-pb28-l1g151 (last visited at April 20, 2009).
[24] *See, generally,* research and materials available at www.ediscoverylaw.com, www.sedonaconference.org, www.edrm.net, www.discoveryresources.org, and other commercial websites and published materials.
[25] *See, generally,* http://www.ediscoverylaw.com/2008/10/articles/resources/updated-list-local-rules-forms-and-guidelines-of-united-states-district-courts-addressing-ediscovery-issues/ (last visited April 22, 2009).

accessible digital information, and can include metadata, encryption keys and other "technical" data not traditionally considered as evidence.[26]

While there is nothing unlawful in the ordinary course of business of disposing of ESI that is not otherwise subject to retention rules, there is a duty to preserve potentially relevant ESI, whether or not the information is otherwise preserved and retained as records.[27] A "litigation hold" is a procedure by which a company notifies its employees and custodians of the duty to preserve relevant ESI and takes steps to identify, collect and preserve responsive materials.

For UC services, it is possible that the legal duty to preserve will apply to many data types (such as transactions data, IM message content, e-mail content, original source files for converted messages) that may otherwise be promptly disposed of in the ordinary course of operating the UC services. As a result, counsel should evaluate the types of controls, processes and records that may be needed in order to implement a "litigation hold". Since many of these data types may be preserved solely for backup purposes, counsel should also evaluate whether the backup data records will be reasonably accessible under applicable laws.

3. Electronic Communications Privacy Act and State "Consent to Record" Laws

In the United States, both federal and state laws regulate the recording of telephone conversations. Largely enacted in the 1980's, these laws present the only true legal hurdle to how effective Internet security services may, or may not, be employed in connection with UC solutions or services. The core questions are how these laws govern, if at all, the capture, storage and use of the digital packets that transport the content of an oral conversation conducted through VoIP or other related UC services. It is not an easy question to resolve (Part IV—The Legal Analysis is entirely devoted to that task), since the relative antiquity of the laws, compared to ongoing technology innovation, requires careful analysis.

To begin, separate introductions to the federal law (Section 3.1) and state laws (Section 3.2) are provided. Section 3.3 offers a detailed review of the defined terms of the federal law (many of which are similarly defined in the state laws) and a survey of the activities expressly permitted by the federal law (and nearly all of the state laws). This review serves as the foundation for the analysis in Part IV of this Report.

[26] *U.S. v. Forrester,* 512 F.3d 500 (Cal. 2008); *see also Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co*., 2009 U.S. Dist. LEXIS 21250 (M.D. Fla. 2009); see also *In re Genetically Modified Rice Litigation*, 2007 WL 1655757 (E.D.Mo. 2007).

[27] Fed. R. Civ. P. 26(a) (initial duty); Fed. R. Civ. P. 26(e)2 (initial duty); *discussed at Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432–34 (S.D.N.Y. 2004); *see also* Fed. R. Civ. P. 34(a)(1)(A) (scope of duty); *discussed at City of Seattle v. Prof'l Basketball Club*, LLC, 2008 WL 539809 (W.D. Wash. 2008); *see also Keithley v. Homestore.com, Inc.*, 2008 WL 5234270 (N.D.Cal. 2008); *see also Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, (S.D.N.Y. 2003).

3.1 Electronic Communications Privacy Act—An Introduction

The Electronic Communications Privacy Act was enacted by Congress in 1986. The same legislation included the Stored Communications Act, and both are often referred to collectively as "ECPA".[28] ECPA updated federal law in order that the legal rights and limits on law enforcement agencies to intercept telephone communications were adapted to then-modern innovations represented by cellular telephones, data transfers between computers, and electronic mail.[29] Congress also was aware of the increasing risks that those operating communication services, and storing related records on computer systems, were confronting: escalating security risks created by those seeking unauthorized access to stored electronic records, including financial data, personal health data, and communication activity records. Congress made that unauthorized access and use unlawful, and provided both criminal penalties and civil remedies for violations. [30]

In 2009, it is difficult to imagine the communications world that existed in 1986. Today, the Internet has emerged as the infrastructure for global communication. The ease with which we can adopt and use the new capabilities and features of unified communications fails to reflect how transformative the changes in communication products and services have been during the last 23 years. With the transformations have also come changes in the diversity and potential impact of the security risks that confront daily use of the Internet for every consumer, business, supply chain of suppliers and network, as well as governments, military operations and educational institutions. Cybersecurity is now a national priority in the United States,[31] and a persistent concern against which corporations commit extensive private resources. Thus, neither the current benefits of the Internet, nor the risks, were at a magnitude anything comparable to what Congress considered in 1986.

Since its enactment, ECPA has not been substantively amended. That relative stability may also be viewed, particularly for a technology-focused law, as stagnation. There is a marked contrast when ECPA is compared, for example, to the Computer Fraud and Abuse Act, a law originally enacted in Congress in 1984, but substantively amended at least five times in order to take account of continuing changes in

---

[28] Pub. L. No. 99-508, 100 Stat. 1848, codified at 18 USC §§ 2510-2521, 2701-2710 and other miscellaneous locations. For this report, additional references will be to applicable USC references. The United States Senate issued a report accompanying the legislation. S. Rep. No. 541, reprinted in 1986 U.S.C.C.A.N. 3555 (hereinafter, the "Senate Report").

[29] Senate Report at 3555. Excellent analyses and detailed descriptions of ECPA's legislative history are found in Dierdre Mulligan, "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557 (2004) (hereinafter "Mulligan") ; and Thomas Greenberg, E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute, 44 Am. U. L. Rev. 219 (1994) (hereinafter, "Note"). Additional papers of interest may be found at the websites of the Center for Democracy and Technology listed in Appendix 2—Legal and IT Resource Inventory.

[30] Senate Report, Id.

[31] As one of his early actions as President, President Obama commissioned an intensive 60-day review of the cybersecurity status of the United States. http://www.whitehouse.gov/the_press_office/advisorstoconductimmediatecybersecurityreview/. Under the direction of Dr. Melissa Hathaway, that review was completed in April, 2009. *See, e.g.,* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=338289 (last visited April 27, 2009).

technology, malicious actors and the needs for different views of security in light of evolutions in terrorism, hacker misconduct and financial fraud.[32] Those changes have also been affecting the boundaries of the activities on which ECPA focuses, but there has been, to date, no responsive legislative reform. Indeed, the present existence of, and future potential for, unified communications products and services highlights even further the potential for tension in applying ECPA to current technologies.

Enabling Protection Against Excessive Search and Seizure Powers

ECPA responded to the technology-driven tension between the controls and limits of the Wiretap Act, first enacted in 1968 as Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[33] and the innovations by 1986 of cell phones, e-mails and computer storage of personal information.[34] Prior to 1968, the courts had confirmed that an individual's constitutional Fourth Amendment protections against search and seizure extended to protect individuals against the government intercepting and reading personal mail without due cause. The Wiretap Act was enacted on the principle that an individual has an expectation that their personal conversations conducted over wire telephone networks (the only means of conducting a conversation in 1968) were as private as their personal mail. Thus, the central legal right toward which the Wiretap Act was focused, as well as ECPA, was controlling excessive actions by government in violation of the Fourth Amendment.

Congress was looking at, and establishing the legal standards for, the expectations of citizens against the attempted exercise of governmental power and its potential abuse. Despite the actual title of the law, ECPA, as an update to the Wiretap Act, was *not* a purposeful expression of an individual's right of privacy as a broad social principle. The more limited focus of ECPA stands in marked contrast to the European Union privacy doctrine that is so challenging to many companies with international operations. It is also in contrast to Congressional activity that has taken steps to protect stored personal information in health care and financial services,[35] as well as state legislative activity to increase the security provided to personal information.[36] ECPA was a contemporaneous update of the Wiretap Act to adapt to changing technology; the law attempted to stabilize a Congressional intent that the Fourth Amendment protected citizens for all of the varieties of electronic communications that were then entering the marketplace.

By 1986, cellular telephone networks, electronic mail and other computer-based information services that used traditional POTS circuits to communicate were recognized as important innovations. Law

---

[32] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act.

[33] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, enacted October 21, 1986.

[34] *See, generally,* both the Senate Report and House Report. *See also* Mulligan, Greenberg and Oza law review articles cited in Appendix 2—Legal and IT Resource Inventory.

[35] Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338, enacted November 12, 1999; Health Insurance Portability and Accountability Act of 1996, Pub. L. No.104-191, Administrative Simplification Sec 261-262, Sec 1171-1179; enacted August 21, 1996, Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, enacted July 30, 2002.

[36] See the discussion in Section 2.2 of this Part IV, *supra*.

enforcement officials were concerned that the Wiretap Act limited their ability to access the content of communications through these new communication services; those seeking to assure the continued validity of Fourth Amendment protections for these new services advocated that that legislative clarity was more appropriate than a series of incremental, and potentially inconsistent, judicial decisions. Similarly, with the increased reliance on computers to store vast amounts of personal information, all stakeholders in the debate were interested in clarifying the extension of the Fourth Amendment to protect a citizen's interests in the stored electronic records, including the content of their electronic communications through these new communication mediums.[37]

In furtherance of that objective, Congress recognized that ECPA needed to refine several definitions in order to better administer law enforcement authority. The new technologies presented several challenges to the defined terms employed in the Wiretap Act, as enacted in 1968. In order for Congressional intent to be effective in defining acceptable and unacceptable activities, old terms needed refinement and new terms needed to be introduced. While Section 3.2 (below) explores the results in detail, it is useful to summarize the problems Congress was trying to resolve with the definitional reforms ECPA put into place:

- Types of communications and data. Congress sought to distinguish between:
    - live, oral communications (for the purpose of regulating listening devices aimed at live conversations).
    - oral conversations occurring through technology (i.e., telephone conversations), distinguishing between
        - the audible portion of an oral conversation (i.e., the analog signal)
        - any digitized version of an oral conversation (such as carried between servers on the networks) (a distinction discussed in Part II of this report)
    - electronic communications containing any digital content *other than* as part of an oral conversation (namely electronic mail, video conferences, computer data, etc.)[38]
    - transactional data used to administer technology-enabled oral and electronic communications and accounting relating to the services.
- Types of equipment and systems. Congress sought to distinguish between:
    - services and systems used for:
        - oral communications.
        - other electronic communications.

[37] *See, generally* Mulligan, Note and Oza law review articles, cited in Appendix 2—Legal and IT Resource Inventory.
[38] Senate Report at 3579.

- services and systems for both oral and other electronic communications "offered to the public"
- services and systems for both oral and other electronic communications privately operated (such as a corporate telephone system).

- Types of activities. Congress sought to distinguish between:
  - intercepting with respect to live oral communications (through listening or recording devices)
    - the content of the communication.
    - the transactional data relating to the communication.
  - intercepting with respect to other electronic communications while in transit:
    - the content of the communication.
    - the transactional data relating to the communication.
  - accessing stored records of the content of (and transactional data relating to):
    - oral communications.
    - electronic communications.
  - storage services operated by:
    - the provider of a communications service
    - remote storage service providers.

ECPA and Current Technologies

In comparing the outcome under ECPA in 1986 and the realities of unified communications in 2009, what is interesting to appreciate is that UC products and services, while enormously different than the mix of technologies that existed in 1986, are not fundamentally different in design. UC solutions have many common denominators with then-extant technologies, thereby enabling a more straight-forward analysis than might be expected:

- UC solutions transport both oral conversations and other electronic communications.
  - Today, the transport of oral conversations generally includes far more transit in digital format, rather than analog, but both were contemplated by Congress in enacting ECPA.

- UC solutions create both substantive content, as well as transactional data necessary to administering the services.
    - Today, the transactional data is more extensive, including significantly more information to process communications through Internet networks, but no different in its essential function or utility.
- UC solutions involve both private companies and public common carriers, as well as storage offered directly by the service provider and remote storage services.

Under ECPA, law enforcement agencies, courts, operators of electronic communication services and the aggrieved users (who believe their rights have been violated by acts of interception or access to stored records) have collectively struggled to adapt the legislative language to the continuing evolving technology. While generalizations should be made with care, a detailed review of the case law suggests that, in nearly every case, the issues have involved either the government or a private entity (usually an employer) acquiring the content of a communication and relying on that content to pursue other legal recourse (criminal investigation, prosecution, employment discipline or termination).[39] That review has not, however, identified any cases in which the court was asked to review the legal status of conduct by an operator of electronic communications facilities (such as cell phone networks, data networks, e-mail servers, text message pagers, etc.) that was solely undertaken to provide security services for those facilities and the related services.

Therefore, it is useful to appreciate what ECPA does, and does not, prohibit. The law provides extensive guidance to the rights of law enforcement to lawfully intercept live communications (also known as "communications in transit")[40], as well as access stored communications. ECPA sets forth, when applicable, the procedural criteria by which judicial authority to conduct such activities can be obtained. There are several excellent law review articles (listed in Appendix 2--Legal and IT Resource Inventory) that review those provisions in detail, focusing specifically on the tensions that have evolved under Constitutional legal theories of privacy and current technologies and practices. But ECPA also expresses what private entities, notably providers of electronic communication services, are allowed to do in connection with access requests by the government and others. Those permissive provisions are analyzed in further detail in Section 3.3 below.

3.2 State "Consent to Record" Laws

The federal provisions in ECPA address *interstate or international* communications. Many states were concerned, following ECPA's enactment, that their citizens and businesses were not effectively protected against the hazards of recorded telephone conversations if the calls involved *intrastate*

[39] Commercial law research services, such as Westlaw or Lexis-Nexis, provide access to all of the case law and related materials. Appendix 2--Legal and IT Resource Inventory identify notable cases of direct value to our analysis.
[40] Mulligan, at note 65.

conversations (in which all parties to a call are within the boundaries of the enacting state). In response, 38 states and the District of Columbia have enacted laws which regulate recording activity.[41]

As a general principle, ECPA and all of the state laws allow recording of conversations with consent. However, while ECPA and most state laws expressly permit interception (i.e., recording) if one of the parties consents, 12 states express a two-party consent rule. But for that difference, nearly all of the state laws track verbatim other aspects of the federal law.[42] In California, the Supreme Court has ruled that California's two-party consent rule applied to interstate communications, even if the call from which a state originated was a one-party consent law.[43]

Whether any required consent must be explicit or implicit (such as continuing to participate in a call that is initiated by a recording "This call may be monitored for quality control purposes") varies somewhat among jurisdictions; generally, any implicit consent should be evidenced by circumstances sufficient to indicate no genuine expectation of privacy for the communication existed. But all of the case law reviewed has focused on "interception" or "recording" in the popular meanings of the term: a physical interception, such as picking up an extension to listen into a conversation, or creating a stored duplicate copy of the audible spoken words in a telephone conversation.

Taken together, the state "consent to record" laws represent a substantive, and fairly stable, body of law. Companies with direct phone solicitation campaigns, online customer services, financial services, etc. are all familiar with these laws and should already have put into place appropriate compliance services (policies prohibiting recording, requiring appropriate consent, providing a "notice of recording" announcement, etc.). As with compliance with the state privacy laws (discussed in Section 2.2 above), the migration of POTS services to VoIP should not trigger any different compliance duties regarding how consent is obtained (or not obtained).

A significant unresolved question under state laws is also a core issue not previously evaluated under ECPA: Will the normal operation of UC services (whether e-mail, IM, VoIP, video or other services), or the use of applicable Internet security services (as described in Part II—Internet Security Services) with respect to the management and routing of the related communications, represent an "intercept" that would be unlawful in the absence of effective consent? Section 4 provides the foundation for that question to be answered in Part IV—The Legal Analysis.

4 Understanding ECPA's Definitions and Permitted Activities

What Congress did not appear to contemplate in the 1980s, based on the related legislative history, was the ease with which live, oral conversations over the telephone could be recorded and stored in digital formats that were not audible per se, but were capable of being accessed and reviewed as audible conversations at a later date. While ECPA recognized that oral conversations could be stored,[44] there

[41] One useful summary of the state consent to record laws is found at http://www.rcfp.org/taping/states.html.
[42] *See, e.g.*, Florida's statute at Fla. Stat. Ch. 934.03.
[43] *Kearney v. Salomon Smith Barney*, 39 Cal.4th 95, 137 P.3d 914 (Cal. 2006).
[44] See the discussion of "wire communication" in Part 2.2 *supra.*

seemed a presumption that oral conversations had no "shelf life"—the law was targeting live, intentional interceptions in real-time of audible conversations.

There is little question under both federal and state laws that an operator of an electronic communications service that stores a recording of any type of communication and then allows humans to "listen" for the express purpose of understanding and acting on the communication content faces legal risk. But, as described in detail in Part II—Internet Security Services, the protective controls and processes applied to any Internet activity, as well as UC services, do not involve humans listening to audible recordings, but software tools analyzing data flows, packet headers and payloads for evidence of malicious activity that can be quarantined or rejected before harm is caused.

4.1 Key Definitions and Questions under ECPA

In any legal analysis, the words matter. This Section presents in depth the architecture of the terms defined by ECPA that are relevant to evaluating how ECPA impacts Internet security services for UC solutions. For each definition, we have included some of the questions that each term might provoke in the minds of any lawyer or technologist that is also trying to evaluate the fit among ECPA, UC solutions and services, and Internet security services. Part IV—The Legal Analysis endeavors to make sure all of those questions are coherently answered.

Consistent with the structure of the problems Congress was trying to solve presented in Section 2.1 above, the key ECPA definitions may be loosely organized into three classes:

- Types of communications and data.
- Types of devices or systems.
- Types of actions or activities.

4.2 Types of Communications and Data

Oral communication means "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication."[45]

- Does the express exclusion of "electronic communication" limit "oral communication" to live, direct conversations not enabled by any technology, devices or systems?[46]

Aural transfer means "a transfer containing the human voice at any point between and including the point of origin and the point of reception."[47]

---

[45] 18 U.S.C. § 2510.

[46] Each of the questions presented in this Section 4 are the types of legal questions a lawyer might ask in conducting his or her own analysis. We have included these questions in order to highlight some of the definitional awkwardness of applying ECPA to 21st century UC solutions. Nearly all of these questions are answered in the analysis presented in Part IV—The Legal Analysis of this Report.

- What is the difference, then, between an oral communication and an aural transfer? Can there be any oral communication enabled by an electronic communication service or electronic communication service (as separately defined below) that is *not* an aural transfer?

- Is a VoIP communication, in which the human voice (an analog signal) is converted into a digital format for transfer and re-converted into an audible sound at the point of reception an "aural transfer"?

- Is a machine-synthesized file converting text to audible sounds (e.g., e-mail to voice) a "human voice" for purposes of the statute?

- Is a machine-synthesized file converting a recorded human voice (such as a voice mail) into text an aural transfer? Is the answer different if the conversion is occurring in real-time, concurrently with the recording, or after the recording is a stored communication?

Wire communication means "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication."[48]

- Note: a wire communication is limited to aural transfers; the term does *not* include any other types of electronic communications.

- Is the Internet a "wire, cable, or other like connection"?

- Is a VoIP communication a "wire communication", whether or not any part of the POTS services are employed?

- Is a corporation operating a facility for internal telephone communications (such as a PBX) doing so for the transmission of interstate or foreign communications affecting interstate or foreign commerce? Is the answer different if the facility enables communications with external parties (customers, suppliers) in connection with commerce?

- What are the implications for including "any electronic storage" as part of a wire communication?

Electronic communication means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[49] An electronic communication cannot be an oral communication or a wire communication; the term is explicitly exclusive.

---

[47] 18 U.S.C. § 2510(18).
[48] 18 U.S.C. § 2510.
[49] 18 U.S.C. § 2510 (12).

- Are normal electronic mail messages and data transfers between computers "electronic communications"?
- Is it possible to transfer an electronic communication that is not transmitted in whole or in part by a wire, radio . . . system that affects interstate or foreign commerce?
- Is the converted signal following the conversion of an aural sound into a digital format an "electronic communication"?

Content includes "any information concerning the substance, purport or meaning of" any wire, oral, or electronic communication.[50]

- Is all transactional data (date, time, duration, sender identification, receiver identification, packet header data, management data and similar information generated and used in UC communications (as described in Part _--Understanding the Internet) "content"?
- Note: Congress did not separately provide a definition for transactional data, but clearly expressed its intent that such information was *not* considered part of "content". ECPA amended the Wiretap Act definition of content for that purpose.[51]

4.3 Types of Systems and Devices

Electronic, mechanical or other device means "any device or apparatus used to intercept a wire, oral, or electronic communication."[52] But, there is a statutory exception that expressly *excludes* from the scope of this definition any device that meets the following four criteria:

- a telephone or telegraph instrument, equipment or facility, or components
- furnished to a subscriber or user by the provider of wire or electronic communication service
- in the ordinary course of business *and*
- used in the ordinary course of business.[53]

[50] 18 U.S.C. § 2510(8).

[51] Senate Report at 3567. The Wiretap Act codified a distinction, first recognized by the Supreme Court in Smith v. Maryland, 442 U.S. 735 (1979), between the content of communications and non-content information. Non-content information, such as transactional data (originating telephone number, date, time, duration of call), was viewed as information for which the participants had no expectation of privacy. Since that type of information was needed to route, process, charge for, and manage the communication, it was considered as information voluntarily placed by the participant into the "stream of commerce" and not protected. As a result, the Wiretap Act imposed few restraints on law enforcement agencies wishing to install pen registers or trap and trace devices on telephone systems in order to capture that type of information from the switches and routers. ECPA continued that approach, but with even greater clarity with the modified definition of "content".

For those in the private sector, that difference between content and non-content data (i.e., transactional data) is important, since it seems to grant to the providers of UC solutions a generous "safe harbor" to use that data in routine operations, including in the ordinary course of performing Internet security services. *See* Part IV—The Legal Analysis.

[52] 18 U.S.C. § 2510(5).

[53] 18 U.S.C. § 2510(5)(a).

This definition has the practical effect, under ECPA, of allowing the provider of a wire or electronic communication service to furnish the devices, equipment and components needed for users to use the services.

- Is a company providing UC solutions to its employees a "provider of . . . [an] electronic communication service"?
    - If yes, are all of the devices required and provided by the company to provide that service (PBX routers, servers, computers, mobile devices, cell phones) considered as "equipment or components. . . furnished to a . . . user . . . in the ordinary course of business"?
        - Could any use of such devices by the company to perform routine internet security services be considered as a use that is *not* "in the ordinary course of business"?
    - If yes, is the normal use of those devices by employees to conduct the business activities of the company "in the ordinary course of business"? Is there a different result if the employee is using the devices for personal purposes (or other uses not relating to the business of the company)?

Electronic communications service means any service which provides to users thereof the ability to send or receive wire or electronic communications.

- Is virtually any Internet-based communication service an "electronic communications service"?
- What, if any, is the practical distinction between a "service" and a "system" (as used in the definition for an "electronic communications system" below)?

Electronic communications system includes:

- any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, *and*
- any computer facilities or related electronic equipment for the electronic storage of such communications.

- Do all systems, computer facilities and related electronic equipment used to provide UC solutions represent "electronic communication systems"?
- Are any devices used to provide routine Internet security services for UC communications *not* part of the electronic communications systems? Can any such devices be considered as "electronic, mechanical or other devices" used to "intercept" UC communications?

4.4 Types of Actions

Intercept means "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[54]

- Is the inherent acquisition and temporary storage of an electronic communication in the ordinary course of transmission and receipt an "intercept"?
- Does an "intercept" require a purposeful use of an additional device not otherwise used in the ordinary course of executing a wire communication or electronic communication?

Electronic storage includes:

  - temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission, and
  - storage of such communication for purposes of backup protection of such communication.[55]

- Is the routine preservation of converted content (e.g., e-mail to voice; voice mail to text) for quality control and audit purposes within the scope of "electronic storage"?
- Is the normal intermediate storage of IP packets making up UC communications (as "electronic communications") "incidental to the electronic transmission"?

4.5 Permitted Activities

While ECPA establishes numerous prohibitions or restrictions on activities by government agencies and persons in the private sector to intercept or access wire communications or electronic communications, as discussed earlier, there are numerous provisions which expressly protect certain conduct by persons in the private sector from being considered as illegal. These provisions are important to evaluating the range of activities a provider of electronic communication systems and electronic communication services can perform. Following is a summary of the key activities permitted to be conducted by non-governmental providers of electronic communication services.[56]

A provider of an electronic communication service will not engage in unlawful conduct (i.e., the following conduct is lawful) if:

A. The provider records the fact that a wire communication or electronic communication was initiated or completed.[57] The recording activity needs to be conducted in order to protect:

- such provider,
- another provider furnishing services toward the completion of the wire communication or electronic communication, or

[54] 18 U.S.C. § 2516.
[55] 18 U.S.C. § 2703.
[56] This Report focuses on private sector operations of UC solutions; the many additional issues relating to governmental activities and the potential tensions between the current legal structures and their impact on future governmental investigative and enforcement authority are outside the scope of this Report.
[57] 18 U.S.C. § 2511(2)(h)(ii).

- a user of that service.

The risks against which protection is to be focused are "the fraudulent, unlawful or abusive use of such service."

B. The provider operates a "track and trace device" in connection with an electronic communication service or wire communication service, relating to:

- operation, maintenance and testing of the service, *or*
- the protection of the rights or property of the provider, *or*
- the protection of users of the service from abuse of service or unlawful use of service, *or*
- recording that a wire or electronic communication was initiated or completed, in order to:
    - protect such provider, another provider or a user of that service
    - from fraudulent, unlawful or abusive use of service.

C. The provider conducts certain interception, disclosure or use of wire or electronic communications. For the conduct to be legal, a provider of a wire or electronic communications service[58], whose facilities are used in the transmission of a wire communication or electronic communication, may:

- through "an operator of a switchboard, or an officer, employee, or agent of the provider"
- intercept, disclose, or use that communication, if:
    - that conduct is in the normal course of his [i.e., the operator, officer, employee, or agent's] employment.
    - while engaged in any activity which is:
        - a necessary incident to the rendition of his service, *or*
        - to the protection of the rights or property of the provider of that service.[59]

Taken collectively, these permitted activities, along with the interplay of the various definitions, construct for a provider of an electronic communications service a substantial "safe harbor" for activities the provider conducts in the normal course of operations. The provider can record details of the communications events, capture the transactions data, and have officers, employees and agents intercept and use communications when in the ordinary course, as a normal incident to the rendition of services *or* in protecting the rights and property of the provider.

[58] Note: the phrase "wire or electronic communication service" is a bit awkward, since "electronic communication service" includes any service which sends or receives wire or electronic communications. Thus the words "wire or" do not appear to add any substantive meaning. *See* 18 USC § 2510(14) and (15).
[59] 18 USC § 2511(2)(a)(1).

In Part IV—The Legal Analysis, we evaluate how that safe harbor sustains the performance of Internet security services for UC communications and related services.

Part IV—The Legal Analysis

Table of Contents

This Part IV relies upon earlier parts of this Report to present a detailed analysis of the interactions between ECPA and effective Internet security services for UC solutions.

- Part II reviewed the Internet security programs that can protect any company using Internet-based services; the security threats and vulnerabilities associated with UC solutions; and the types of security services that can be effective in assuring that UC solutions are not the source of

direct losses of property, service disruptions or interferences with the rights of the company or its employees.

- Part III of this Report surveyed the tapestry of call consent, privacy, e-discovery, information security, FCC orders and ECPA laws that are the principle features of the legal landscape for unified communications. The analysis emphasized that, while all of these laws require consideration, only ECPA required detailed legal attention in determining whether applying effective Internet security to UC solutions and services is lawful.

Our analysis in this Part IV examines the following core questions:

- Does ECPA present an obstacle to the efforts of companies in the private sector to secure their networks, systems and devices against malicious actors?

- Does ECPA limit the use by companies in the private sector of Internet security services to protect a company's systems and devices against the persistent and hazardous risks of the Internet?

- Does ECPA, a federal law designed itself as an accommodation between different generations of communications technologies, interfere with or handicap the full potential of contemporary or foreseeable UC solutions to integrate and transform traditional separations between voice and electronic communications?

While the following analysis will be of interest to anyone implementing UC solutions, our primary audience are the lawyers who will be asked to provide their opinion on the preceding questions. Our objective is to share with them the reasoning and precedents in sufficient detail to allow them to independently serve their clients.

Summary

We believe independent legal counsel can reach a confident conclusion that ECPA is *not* a barrier to the use of Internet security services by companies that provide UC solutions to their enterprise. Nor does the Stored Communications Act preclude companies from storing, accessing and using the stored content of communications transmitted through UC solutions in the ordinary course of performing forensic investigations, security analyses, quality of service audits and other routine information security management services. *However*:

- Any access obtained to the audible version of a recorded wire communication that would otherwise require consent under state mutual consent-to-record laws should not be permitted (unless appropriate consents are obtained).

- Any voluntary disclosure of the content of stored communications to others, or any use of stored communications in a manner that would offend the principles reflected by the call consent laws, should only occur after careful legal analysis.

While there are some delicate legal alignments needed between the overall federal legal framework for electronic communications and current technologies, those alignments do not rise to the level of making illegal the use of security controls and processes that serve to protect the systems, properties and rights of the enterprise and its employees against criminal misconduct, fraud, abuse, unauthorized access and malicious activity.

Our analysis follows in a series of detailed questions and answers. We have included in the footnotes to our analysis references to relevant cases, law reviews and legislative history, sources which could serve as possible precedent should the questions we present arise in formal litigation. These sources are also useful starting points for more detailed research that a company or its counsel may wish to conduct.

We have organized our analysis around the two activities that are the focus of ECPA (and the Stored Communications Act; the "SCA"), namely (a) the interception and use of wire and electronic communications, and (b) access and use of stored records of wire and electronic communications. It is important to emphasize that ECPA and SCA were enacted to protect communications *in the course of transmission*.[1] Thus, our analysis actually focuses somewhat narrowly on the time periods and activities associated with transmission, and the ability of companies to perform Internet security services during and in connection with those activities. The long-term management of any recorded communication (or related transactional data) is better considered as part of the records management programs of an enterprise.

Interception of Wire Communications

How are the following content items classified under the ECPA definitions?

- "Electronic communication" includes all of the following types of communications that are created, transmitted, managed and stored by UC products and services used by businesses. Each of these are clearly within the broad scope of the definition for "electronic communication", which seeks to include virtually any electronic content that "cannot fairly be characterized as containing the human voice."[2] (*see* Part III—The Legal Landscape, Section 4).
    - *Electronic mail.*
    - *Instant messaging or chat text.*
    - *Video images and sounds that are not separately identifiable as wire communications* (i.e., aural transfers in conversation).

[1] *See Fraser v. Nationwide Mut. Ins. Co.*, 135 F.Supp.2d 623, (E.D.Pa.,2001); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002); *see, generally*, Part III—The Legal Landscape.

[2] Senate Report at 3568. As a Rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in part by wire)." House Report No. 99-647, at 35 (1986). *See also United States v. Councilman* , 245 F. Supp. 2d 319, 320 (D. Mass. 2003) (definition of electronic communications is "extraordinarily – indeed, almost breathtakingly – broad").

- *Documents or files that are writings or contain data or "intelligence of any nature."*[3]

- *Any file representing an audio recording of text that has been generated by automated methods (e.g., e-mail synthesized by computer into audio)*.

  Since "electronic communication" expressly *excludes* any wire communication (see the following paragraph), VoIP communication content, whether as an analog signal or in a digital format, is not an electronic communication. However, "electronic communication" reasonably includes any file representing an audio recording of text that has been generated by automated methods (e.g., e-mail converted to audio). ECPA clearly distinguishes between human conversation, providing separate and connected definitions for oral communication, aural transfer and wire communication, while also allowing that "electronic communication" includes any other sounds.

  The author of an electronic mail, IM or other text content is not "speaking" and, therefore has no expectations of privacy that are normally associated with oral conversations (*see* Part III—The Legal Landscape). The fact that a receiver has configured their electronic communication system to re-format a text file into an audio recording does not change those expectations.

- "Wire communication" includes the following:

  - *VoIP content*, including (a) the audible human voice of a normal conversation occurring through the use of VoIP services, and (b) any digital conversion of such audible voice that is created and transported across wire or comparable facilities.

    This classification is based on three points, taking account of the qualifying elements of the definition of a "wire communication":

    - The first criteria is that there be an "aural transfer", which in turn requires "a transfer containing the human voice *at any point between and including* the point of origin and the point of reception." Since VoIP services involve the capture of the human voice (as an analog signal) at the point of origin for each participant in the communication, any VoIP conversation is an "aural transfer".

    - The second criteria is that facilities be used for the aural transfer, in whole or in part, that evidence the following features:

      - "by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station). . . "

[3] 18 U.S.C. § 2510(12).

While this language was clearly intended to include the telephone systems extant in 1986 (the enactment date for ECPA), the words are not expressly limited to those systems. Instead, the emphasis is on the existence of a physical (versus wireless) connection at some point between the origin and reception points. The fact that intervening systems may allow for some portion of the transmission to move through wireless transport of the aural transfer did not exclude the overall characterization of the communication as a "wire communication".

The Internet has many wireless components, but the central systems employed, and the end points through which many users access the Internet involve "wire, cable or like connection". Thus, it is reasonable to conclude, for the purpose of this criteria, that any voice communication transported across the Internet is a wire communication.

It is useful to also appreciate that, for those formulating public policy that was aimed, in part, at protecting citizens against improper monitoring by law enforcement of their conversations, an oral conversation occurring through VoIP appears to them (and the user) like any other telephone conversation. Indeed, VoIP service providers have established inter-connections with POTS services in order that conversations can be transferred between their technologies. A participant in a conversation brings to a VoIP enabled communication the same level of expectation of not being subject to interception as to a normal telephone call.[4]

Indeed, the ECPA legislative history expressly stated that the 1986 amendments intended to make illegal the interception of "the non-voice portion of a wire communication, such as the digitized portion of a voice communication.[5]

- The third criteria is that the facilities used be furnished or operated by:
    - any person engaged in providing or operating such facilities for the transmission of:
        - interstate or foreign communications, or

[4] *See* the definition of "oral conversation," 18 U.S.C. § 2510 (12)(B).
[5] Note, at 233 and note 77, citing Senate Report at 3567 and 3589.

- communications affecting interstate or foreign commerce.

Based on prior judicial decisions considering ECPA's applicability to a variety of activities by employers (or their agents) involving their monitoring of telephone communications by their employees, the courts clearly embrace the perspective that communications facilities operated by a company engaged in commerce meet the definition threshold of this criteria.[6] Indeed, because of the Internet's global reach, companies operating facilities connected to the Internet are often actively communicating both on an interstate and foreign basis.

Clearly "commerce" must be affected, and there could be some basis to conclude that university, academic or government facilities would not meet this criteria. However, for all other companies engaged in business, there is commerce at stake with respect to any communications they conduct.[7]

> Note: While corporate employees will, of course, use communication facilities for personal purposes, unrelated to the commerce in which their company engages, it is established practice in the United States that a company's technology usage policies (including for telephone, Internet and e-mail) specify that employees can have no expectation of privacy, and that the content of all such communications is available to the company for monitoring. Therefore, we believe it is appropriate to treat all conversational traffic similarly.

The definition covers any person engaging in or providing such facilities. In being so constructed, it does not limit its applicability to "communication common carriers", such as telephone companies. Indeed, that term is separately defined[8] and, in electing to not employ it, Congress intended its potential applicability to private networks.[9] Since 1986, courts have consistently viewed the telephone and communication systems operated by companies as within the purview

[6] *See Quon et al. v. Arch Wireless Operating Co. Inc*., No. 07-55282, 2008 U.S. App. LEXIS 12766 (9th Cir. Jun. 18, 2008).
[7] A similar argument of exclusion could be made for those facilities that operate entirely and exclusively on an intrastate basis, but it is difficult to imagine any business operating under those circumstances.
[8] 18 U.S.C. § 2510(10) adopts the definition of "communications common carrier" set forth in Section 3 of the Communications Act of 1934.
[9] *See* Senate Report at 3556-57.

of their jurisdiction to evaluate whether interception or monitoring conducted on those systems was lawful under ECPA.[10]

- *Any file that is a stored version of a VoIP communication.*

  Since a VoIP communication is a wire communication, ECPA expressly includes that a wire communication includes "any electronic storage of such communication."

- *Any file representing a text or similar translation of an aural transfer occurring concurrently with the conversation (e.g., text displays of an oral conversation, such as TTY or TTD services offered to hard-of-hearing or deaf persons).*

  The treatment of these files as wire communications is distinguished from text conversions of an audio recording that occur following the conclusion of the conversation (i.e., an aural transfer). TTY and TTD services exist to enable conversations executed between audible voice and text communicators; as such, the text files are part of the conversation and, therefore, reasonable to treat in that manner.

- A file representing a text conversion of an audio recording that has been generated by automated methods (e.g., voice mail synthesized by computer into text) could fairly be characterized as both a wire communication, for the original communication included the human voice, or an electronic communication since the synthesized result is no different than an e-mail. However, provided no human review of the audible recording is occurring in the conversion, either characterization appears to present no difficulties in analyzing the lawful nature of Internet security services employed.

- One of the noteworthy results of our research was the apparent absence of any judicial decisions that have considered whether electronic mail represents an "electronic communication". This is somewhat surprising in light of ongoing journalistic coverage of the risks of electronic mail and the use of security controls against those risks.

  However, the absence of any legal challenges may actually suggest a more practical reality—unlike our expectations of privacy for normal telephone communications, we have come to expect that our electronic mail *is not private*, at least for the purposes of security controls being employed to protect the rights of the operator of related services. That insight seems equally applicable to virtually any of the UC solutions currently in the marketplace—when there is knowing use of the Internet, we have adjusted as users to the expectation that security controls will be used, and that such use does not constitute a legally suspect action.

[10] *See Quon*, 2008 U.S. App. LEXIS 12766.

How are the following systems, equipment and device items associated with UC products and services classified under the ECPA definitions?

- "Electronic communications service" includes:
  - *Any unified communications services.*

    UC services provide to users the ability to send or receive wire communications *or* electronic communications. Regardless of the actual communications activities supported, virtually any UC service generates either or both classes of communications. This includes:

    - Electronic mail.
    - VoIP content.
    - Instant messaging or chat text.
    - Video images and sounds that are not separately identifiable as wire communications (i.e., aural transfers in conversation).
    - Documents or files that are writings or contain data or "intelligence of any nature."
    - Any file representing an audio recording of text that has been generated by automated methods (e.g., e-mail synthesized by computer into audio).

- "Electronic communications system" includes:
  - *All facilities used for transmitting UC content representing electronic communications (emphasis added).*

    The language of the statutory definition is expansive, including "any wire, radio, electromagnetic, photooptical or photoelectronic facilities." There is little question that UC solutions require and operate through such facilities.

    The statute, however, does *not* indicate that facilities used to transmit wire communications are expressly considered as those of an electronic communications system. This omission may be inadvertent, since other statutory language (specifically, the terms describing interception activities that are not unlawful[11]) references "wire or electronic communication systems" as if the term "wire communication system" had been otherwise defined.

[11] *See* 18 U.S.C. § 2510(2)(a).

- *All computer facilities and related electronic equipment used for the electronic storage of such communications.*

  This inclusive treatment of electronic storage facilities emphasizes the broad scope of "electronic storage", including both:

  - temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission, and
  - storage of such communication for purposes of backup protection of such communication.[12]

  However, because "electronic storage" is defined by the statute, it should not be interpreted to have a broader meaning more inclusive of other data storage activities or purposes. As a result, the storage of communications that may occur for other business purposes, including records management, regulatory compliance, discovery in litigation, quality of service audits, and forensic investigations should not be considered as "electronic storage" under ECPA, nor should the systems and computers used for such business purposes be considered part of the electronic communications system through which those communications are created, transmitted and completed.

- "Track and trace device" includes:

  - *any equipment used to support UC services or as part of the related systems or services, such as routers, servers or flow management devices, to identify the originating number of an instrument or device from which a wire communication or electronic communication was transmitted.*

    In 1986, Congress recognized that networks, and temporary network addresses, were important to electronic communications. In fact, the SCA expressly identifies "temporarily assigned network addresses" as part of the information that must be disclosed by a provider of an electronic communication service, thereby acknowledging that such information is collected and stored in the ordinary course of business as a normal incident to providing the service.

    Today, routers and servers are indispensable to electronic communication. Their function in identifying the source of communications, and executing appropriate routing of that communication is inherent to the operation of packet-switched networks. While far more sophisticated than "track and trace devices" that existed in 1986, the essential function is the same.[13] There

[12] *See* 18 U.S.C. § 2510 (17).

[13] 18 U.S.C. § 2511(2)(h) provides that it is not unlawful to use a trap and trace device, and makes a special emphasis that it is not unlawful "for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from

certainly is no indication in the legislative history indicating that the definition was intended to exclude other types of devices.

How is a company that provides UC solutions to its employees and agents classified under ECPA?

ECPA makes repeated references to a person that:

- "provides an electronic communications service";[14]
- "provides a wire or electronic communications service"; or
- "an officer, employee, or agent of a provider of a wire or electronic communications service."[15]

Additional statutory language directly differentiates those who provide an electronic communications service *to the public*,[16] confirming that Congress intended the references to providers to include privately operated networks and services.[17] Thus, a company that provides UC solutions should be considered as a person that provides an electronic communications service. If the UC solutions include VoIP (or other communications more properly classified as wire communications), then the company is a provider of a wire communications service.[18]

There seems to be no basis for distinguishing in any legal analysis between (a) a company that acquires and owns the hardware, software, computers and other devices that operate a wire or electronic communications service, and (b) a company that licenses, leases or contracts for any or all of the wire or electronic communications service to be provided by a third party. Neither is doing so in order to offer the service to the public. Indeed, the language "or agent of a provider" suggests that Congress contemplated a third party, properly authorized, could act on a provider's behalf.

---

fraudulent, unlawful or abusive use of such service." Such recordation activity is a routine function of Internet security services.

[14] 18 U.S.C. § 2518(11).

[15] 18 U.S.C. § 2511(2)(a)(i).

[16] 18 U.S.C. § 2511(2)(a)(i)(C).

[17] *See* Senate Report at 3565, stating "A private telephone system established by a company whose activities affect interstate commerce, would also be covered."

[18] The term "wire communications service" is not separately defined by ECPA; however it is clear, particularly from 18 U.S.C. § 2510(2)(a)(i) that Congress intended to grant to such persons express rights to conduct certain interception and usage of wire communications in manners that would not be unlawful under the statute.

What actions may a provider of an electronic communications service or wire communications service lawfully conduct that might otherwise be considered as illegal interceptions or uses of wire or electronic communications?

In enacting ECPA, Congress extended to private communication providers certain statutory "safe harbors" for certain interception and uses of wire communications and electronic communications.[19] These "safe harbors" are vitally important, and appear to comfortably safeguard the use of Internet security services that may otherwise be vulnerable to classification as illegal interceptions or uses of UC communications or related records.

There are additional provisions of ECPA that are consistent with the provisions analyzed below[20]; collectively these provisions further protect those who endeavor to intercept computer trespassers or transmissions which are causing harmful interference, as well as those acting "under color of law" in conducting lawful investigations of computer trespassers.

All of these provisions—the express "safe harbors" discussed below and the additional provisions—reflect a consistent Congressional intent that limitations of interception and use of wire and electronic communications should not prevent the providers of the related services from administering their business and protecting their facilities, property and rights—as well as their users and other related providers.

As discussed previously in Section 4 of Part III—The Legal Landscape, there are three classes of activity which ECPA specifically describes as "not unlawful" and which are directly relevant to applying Internet security services to UC solutions—for two classes, there are qualifying conditions, discussed below in further detail. Additional analysis explains how these activities relate to or enable Internet security services to be performed.

The permitted activities are presented in a logical sequence, reflecting the general order in which the related activities occur with any Internet-based communication:

- *Using a device to capture the electronic information that identifies the originating device from which a wire communication or electronic communication was transmitted.*

  Analysis: Capturing identifying information for an originating device (such as any temporary network or IP address) enables security services to be executed based on that information. Those security services include:

  - Identifying and confirming the originating device against lists of approved IP addresses.

[19] The Congressional intent was quite explicit. 18 U.S.C. § 2511(2)(a)(i) substituted "a provider of wire or electronic communications service" for "any communication common carrier". Pub. L. No. 99-508, 100 Stat.1848, 1851. *See also* Note, at 237 (and text accompanying note 90).

[20] *See, e.g.,* 18 U.S.C. § 2511(g), 18 U.S.C. § 2511(i).

- Blocking inbound communications from known hostile IP addresses.
- Proper billing and collection for the related services.

- *Recording the fact that a wire communication or electronic communication was initiated or completed.*
  - To be "not unlawful", the recording activity must be performed in furtherance of protecting either (or all of):
    - the provider.
    - another provider performing services toward the completion of the wire or electronic communication.
    - the user of the related wire or electronic communication services.[21]

  Analysis: The normal management of any Internet-based communications requires this type of recording as a routine part of administering security services that provide protection of the providers and users that are described. Information regarding the initiation and completion of communications activity (wire or electronic) can be relied upon for a wide range of protective activities, including:

  - blocking unauthorized use of the available service.
  - limiting use of the available services to specified time periods, duration, or length.
  - identifying inbound communications that must be further analyzed for security purposes.

  The U.S. Supreme Court, in *Smith v. Maryland*, 442 US 735 (1979), confirmed that the type of information involved in addressing and routing electronic communications is placed by the user into the stream of commerce and, therefore, not subject to the expectations of privacy that might be asserted with respect to the substantive content of a communication itself.[22]

[21] 18 U.S.C. § 2510.

[22] ECPA does nothing to change the reasoning expressed by the Court. Permitting the use of trap and trace devices confirms this routing information is viewed differently in terms of the expectations of privacy. More recent judicial decisions, following ECPA's enactment, continue to affirm the vitality of the reasoning in *Smith v. Maryland. See, e.g.***,** *U.S. v. Forrester*, 512 F.3d 500 (Cal. 2008.) (e-mail and Internet usage), *Morano v. Slattery*

- *Intercepting, disclosing or using wire communications or electronic communications for which the facilities of a wire or electronic communications service are used in the transmission.*

  - To be "not unlawful", the activity:

    - must be performed by an operator of a switchboard, or an officer, employee or agent of a provider of wire or electronic communications services.

    - the provider's facilities must be used in the transmission.

    - the interception, disclosure or use must occur in the "normal course of the employment while engaged in any activity which is a necessary incident to *[either]*

      - the rendition of his service, *or*

      - the protection of the rights or property of the provider of the services.

  Analysis: The statutory criteria serve to expose to potential liability any interception or use of communications that occurs outside the normal course of employment. An example of that type of behavior might be an employee who may be "snooping" for information on a potential inside competitor for a promotion. But, when focusing on legitimate Internet security services, nearly any activities that can be contemplated as potential interception or use are going to be authorized by the provider/employer to be taken as part of the employment of those performing the services and performed in order to achieve improved protection of the rights or property of the provider of the services, as well as the user participating in the wire or electronic communications.

  Following this paragraph are several examples of security services that might be performed with respect to wire or electronic communications conducted as part of UC services. With respect to each, it is worth emphasizing that the services being performed, while occurring under the control of an individual person operating in the normal course of their employment, are largely automated, are integrated into routine, ongoing system management services and are generally completed within a few milliseconds of time.

Skanska, Inc., 846 N.Y.S.2d 881 (N. Y. Sup. Nov 28, 2007) (cell phone call records); *Hause v. Commonwealth*, 83 S.W.3d 1, 11-12 (Ky.Ct.App.2001); *In re Forgione*, 49 Conn. Supp. 613, 908 A.2d 593, 607-08 (Super.Ct.2006).

The interception and use required to perform these security services involves no human activity to listen to a communication; indeed, many of the activities are occurring with respect to individual packets or packet streams, and are not actually interacting with any version of the communication that is audible to the human ear (for example, the converted analog signal that is delivered following the completion of a spoken word).

This distinction appeared to matter to Congress. For example, while providers of wire communication services *to the public* are prohibited from routine observation or random monitoring of communications, except for "mechanical or service quality controls checks", no such restrictions are imposed on privately operated wire communications services or any electronic communication services.[23] Congress seemed to appreciate that the providers of those services had legitimate interests in conducting system monitoring activities that needed to be accommodated. Similarly, Congress appears to have concluded that the expectations of interception for users would also be different with any communication services they would use other than wire communications provided *to the public*.

Internet Security Services for Unified Communications

The following are examples of security services a provider could apply to wire or electronic communications transmitted within UC solutions or services, and their utility in achieving security objectives of the provider.

- Capture and scan the IP address associated with the initiation of a SIP session.
  - Doing so enables a provider to:
    - validate the address is not a known malicious address.
    - approve the address against known or trusted addresses.

    Restricting the inbound communications protects the systems of the provider against potential threats that may originate from malicious actors, as described in Part II—Internet Security Services.
- Scan the payload of an inbound IP packet to identify the type of communication being received (data, voice, video).

[23] 18 U.S.C. § 2511(2)(a)(i). The Senate Report expressly recognized that these provisions took account of the fact that routine system monitoring necessary to the proper functioning of the service did not involve "human listening in on voice conversations. Senate Report at 3574. *See also* Note at 237 and accompanying notes.

- Doing so enables a provider to route the packets to the proper port and server for further routing, storage and processing. Improperly routed packets, of course, disrupt and degrade the operations and systems of a provider.

- Note: Malicious actors will also attempt to fool scanning tools in order that a payload containing malicious code may be routed, improperly, to a harmful destination within the provider's network, systems or computer devices. Scanning helps detect suspicious patterns or errors in payload identification codes.

o Scan the flow of IP packets designated as part of one communication in order to detect irregularities in the payloads that may represent malicious code, links or attachments in violation of corporate procedures (e.g., many companies operating IM services will prohibit links or attachments). Suspicious packets can be automatically rejected or quarantined before proceeding closer toward the target device.

- Doing so protects a provider and its property against the adverse consequences of the irregularities impacting operations.

In reviewing the preceding analysis, one set of security services deserves to be emphasized—the use of scanning tools, filters and other analytical devices to directly scan the packet payload of VoIP or similar aural transfers occurring through UC solutions or services. Absent the downstream conversion of those digital packets into an analog signal, the security devices are not capable of "listening" to the content as such. These devices, collectively, are targeting the payload of IP packets carrying digital content.

While, as digital packets, they are not containing audible content, as such, the related communication is still a "wire communication".[24] But the express "safe harbor" provided by ECPA allows the provider of a privately operated wire communication service to perform the described interception and use activities. That result seems entirely consistent with the overall balances Congress was attempting to strike in terms of when, as between (a) any participant to a wire or electronic communication and (b) the provider of any private wire or electronic communication service used for such communications, any expectation against interception might exist. Simply, such expectations are not contemplated and Congress provided a substantial statutory framework in which the providers may perform legitimate security services.

Nevertheless, those concerned about the expectations of participants in the communications should take some reassurance that the security services do not, in fact, enable any person to "listen" to their communications. Indeed, the more likely risk of interception is by malicious actors who exploit security vulnerabilities across the facilities of other intermediate providers.

[24] *See* Part III—The Legal Landscape, Section 4.

Of course, when SRTP protocols are employed, the related UC communications are protected against that type of functional "listening" as well.

If interception of a wire or electronic communication by a provider of wire or electronic communication services is not unlawful, are there any limits on the subsequent use or disclosure of the intercepted content by such provider?

ECPA does not establish any such limits; however, any specific company may be subject to other legal duties that would limit their disclosure or use of lawfully intercepted communications. Privacy rules, employment agreements, service contracts, judicial orders—all could limit disclosure or use in different circumstances. Absent those types of duties being present, there are no restrictions on any subsequent activity. Indeed, many Internet security services rely upon stored communication records to conduct Internet security services such as forensic analysis, pattern recognition relating to improper routing or port addressing, etc.

Access and Use of Stored Communications

As discussed in Part III—The Legal Landscape, Congress made an important distinction between the interception and use of wire or electronic communications, and access to and use of communications in electronic storage. As discussed above, an employer that is a provider of a wire or electronic communication service has a substantial "safe harbor" in which to conduct interception activities, and to make subsequent use of the stored communication.

However, if a wire or electronic communication is not intercepted concurrently with, or incidental to, the communication, but is merely routed into electronic storage, what are the rights of a provider of the related communication service to access and use the stored communication? This question is particularly important when the provider's access is in furtherance of legitimate and authorized Internet security services routinely performed in the ordinary course of business It is entirely possible that a provider may elect to not apply content filters or scans against the payload content of certain types of communications, particularly if those are being received into the corporate network exclusively through a trusted third-party service provider.

As part of ECPA, the Stored Communications Act sets forth the boundaries of permissible access and use of stored communications. For providers of UC services, those boundaries are not, in our opinion, substantial barriers to performing Internet security services that require access and use of the stored communications.

May a provider of UC services access content of wire communications or electronic communications in electronic storage?

Any person authorized "by the person or entity providing a wire or electronic communications service" is permitted to access communications in electronic storage.[25] Since UC services can be considered as wire communication or electronic communication services, then it only remains for the provider ("person or entity"; *i.e.*, the company providing the UC services) to assure there are suitable authorization policies and procedures, and appropriate documentation of authorization, for access to be lawful.

Which stored records of wire or electronic communications can be accessed?

The Stored Communications Act, in defining what constitutes "electronic storage", imposes limits on when stored wire or electronic communications can be accessed. The statute expressly identifies two circumstances in which records are considered in electronic storage, namely:

- any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
- any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

For Internet security services being performed immediately with respect to live communications, the first circumstance closely aligns to the needs of those services. Indeed, a federal court concluded (in 2003, closely contemporary with current technologies) that nearly any presence of an electronic communication in the random access memory of a computer or a hard drive, however momentary, establishes "storage" (thereby allowing access to be valid, if authorized by the provider, rather than unlawful interception).[26] Such activities are clearly gaining access incidental to the electronic transmission of the wire or electronic communication.

The second circumstance, allowing access for the purposes of backup protection, also aligns to the realistic need for providers of electronic communication services to be able to restore the availability of communications following any type of incident for which the backup copies are preserved. But this second factor has some limits:

- as drafted, the backup option extends only to electronic communication services (which, by definition, do not include wire communications). This exception seems logical, based on then-current technologies when the law was enacted; however, strictly interpreted, it would appear that a provider could not access stored wire communications for backup protection purposes. Practically, that may be an exception without significance, as it is hard to imagine who

[25] 19 U.S.C. § 2701(c)(1). *See also* Note at 237 and accompanying notes.
[26] *U.S. v. Councilman*, 245 F.Supp.2d 319 (D. Mass. 2003).

might object when such access was obtained in connection with a backup reliance scenario.

- Backup services are, by design, only intended to be relied upon to recover and restore data and records required in connection with active computing services disrupted by disasters or other adverse events.[27] Once the communication is completed, then the Stored Communications Act has no further applicability, and imposes no limits on access.[28]

May providers of wire or electronic communication services access stored communications other than when they are in "electronic storage" as defined by the Storage Communications Act?

Under federal law, yes. However, the state consent-to-record laws may restrict that activity for audible voice/wire communications; the ability to access and use those recordings that is one of the primary activities against which those laws are targeted.

The Stored Communications Act imposes no limits on providers of wire or electronic communication services from accessing stored records following the completion of the transmission and the expiration of a time during which backup access may be required.

Security professionals regularly access communication records for a portfolio of legitimate business purposes incidental to operating the communication services and protecting the property, systems and rights of their company. These activities include acting to verify the accuracy of functional controls (such as lookup and validation of IP addresses), investigating possible suspicious patterns in IP addresses, designated ports, or other routing data, as well as confirming the effectiveness of payload filters programmed to detect malicious code or prohibited content (such as attachments or hyperlinks).

These activities are part of quality information security management services. Also, these activities enable providers of the wire or electronic communication services to evaluate the effectiveness of current security controls and inform how to structure and implement continuing improvements.[29] Our research has not identified any basis in the legislative history

[27] *See, generally,* Seymour Bosworth & M.E. Kabay, *Computer Security Handbook,* Chapter 41 (Wiley, John & Sons, Incorporated) (2009).

[28] This reading of the scope of the SCA was confirmed in *Fraser v. Nationwide Ins. Co.,* 135 F. Supp. 2d 623 (E.D. Pa. 623 2001), in which the court observed, "retrieval of a message from post-transmission storage is not covered by the Stored Communications Act." In *Quon,* 529 F. 3d at 902, the Court enforced the Stored Communications Act against a text messaging service provider who continued to "archive" messages that had been delivered to the user, concluding "it is clear that the messages were archived for 'backup protection'". That interpretation seems strained, since archiving is a very different function than supporting potential backup needs. Nevertheless, in that case, the Court's ultimate objection was that the service provider disclosed the content of the messages to someone other than "the addressee or intended recipient", thereby violating the privacy expectations.

[29] *See* Part II—Internet Security Services of this Report. ISO Standard 27001 emphasizes the need for conducting such ongoing review in order to effectively manage information security.

or judicial decisions relating to the Stored Communications Act that suggests such activities, to the extent they rely on accessing stored communication records, were intended by Congress to be considered as unlawful.[30]

Indeed, other provisions of the Stored Communications Act suggest Congress had no interest in such long-term storage, or in limiting the rights of providers to access the related communication records. The principal prohibition of the SCA, § 2701(a), only calls for punishment when unauthorized access is obtained to wire or electronic communications "in electronic storage".[31] In other words, Congress did not enact the SCA to address the access rights (or limits on access) of providers of wire or electronic communication systems to the records of communications transmitted through their services, once the transmission is functionally completed.

That outcome is harmonious with other aspects of the SCA that govern law enforcement authorities seeking access. Recall that Congress, in enacting ECPA and the SCA, was attempting to balance the Constitutional protections against unwarranted searches with changing technologies.[32] In doing so, Congress apparently concluded that an individual's expectations against interception of, or access by government to, their electronic communications declined over time. As a result, after 180 days, law enforcement must meet a much lower standard in securing authorization to access stored communications.

May a provider of an electronic communication service voluntarily disclose to third parties the contents of communications in electronic storage?

Under the SCA, disclosures to third parties of wire or electronic communications held in electronic storage have received significant judicial scrutiny. Voluntary disclosures by a provider of electronic communication services (i.e., those not made pursuant to a warrant or other legal order, for which other statutory provisions provide detailed guidance) are generally prohibited under 18 USC § 2702. As a result, any voluntary disclosure should only occur with careful legal analysis in advance to determine whether the available statutory exceptions, and case law, permit the disclosure.

The courts have reviewed disclosures by employers of the communications of their employees, as well as disclosures by third-party service providers (notably disclosures by the provider to the corporate employer of a communication addressee, where the employer is also the provider's direct customer). The cases are numerous, and sometimes difficult to reconcile, and the results have often been unfavorable for the disclosing entity.

A 2008 court decision held a third-party service provider who had "archived" the content of previous text messages, and then disclosed those records to the employer/subscriber to a text

[30] *See* Appendix 3—Research Method and Notes; *see also* Senate Report at 3584 and House Report at 3598.
[31] See the full text of Sec. 2701 in Appendix 1 of this Report.
[32] See discussion in Part III—The Legal Landscape.

pager service for its employees, had accessed messages held for "backup protection". That determination contradicts, without explanation by the court, other decisions under ECPA and the SCA that consider the backup process is completed at the time the transmission is completed.[33] As a result, the messages that were disclosed were considered by the court to been retained "in electronic storage", thereby triggering the prohibitions of 18 USC 2702.[34] In that case, the court carefully evaluated whether the employer's policies on the ownership, rights of access and use of the content of the messages applied to the text messaging technology in issue, and concluded those policies did *not* properly negate the employee's expectations of privacy.

In performing Internet security services on stored communications, companies should use care in making any voluntary disclosures to third parties. Whether the stored records are held pursuant to prior interceptions that were not unlawful, held for backup protection, or held pursuant to other legitimate business policies or legal requirements (including records retention protocols, regulatory preservation duties or in connection with pending litigation), companies should endeavor to perform the security services on the stored record without making any voluntary disclosures.

If the company directly operates the wire or electronic communications service, and stores the related communications, the performance of the security services should be reasonably straightforward. To the extent the company engages any third party to perform the security services on their behalf, appropriate contract language and operating controls can be put into place that protect whatever expectations of privacy may exist in the substantive content of the stored communications.

For those companies that have contracted with a service provider to operate a wire or electronic communications service for the company, and that service provider maintains the stored copies, the performance of the security services should be orchestrated in order that the content of the stored messages held by the service provider are not voluntarily disclosed to the company.[35]

Part V—Practice Toolkit includes suggestions on policies a company could develop that would reduce the likelihood that any of the voluntary disclosures just described would provide to an employee or other user any continued expectation of privacy in the communications.

How should recordings of aural transfers or other human voices be managed under a company's records and information management program?

[33] *See, e.g.*, *Theofel v. Farey-Jones*, 359 F.3d 1066 (C.A.9, 2004).
[34] *Quon*, 529 F.3d 892.
[35] This caution appears to be unnecessary for any voluntary disclosure of the identifying information and communication record data (date, time, duration, etc.) that may otherwise be stored; however, our research did not identify any cases in which the voluntary disclosure was limited to such data.

A company's records management program should establish appropriate classifications for each type of record or data asset that is created through the use of the UC solutions or services. While this step seems fairly obvious, many companies overlook the importance of establishing appropriate retention and destruction rules for communication assets (electronic mail, IM, voice mail, aural transfer records, etc.) as well as data assets maintained to assure computing continuity (i.e., backup tapes). As a result, many of these data assets are retained, and poorly managed, much longer than necessary to support the required services or backup needs. Many of the e-discovery quagmires facing companies today originate in their poor historic management of these types of data assets.

Consistent management of UC records and security performance data through the records management program also helps assure that these assets, for the time period they may be retained, are protected with the appropriate controls that can limit access, disclosure or use only to those authorized employees or agents designated for that purpose. Doing so helps protect against any disclosure or use that would not be within the "safe harbor" discussed in this Part IV or other legal restrictions (such as privacy rules).

Part V
Practice Toolkit

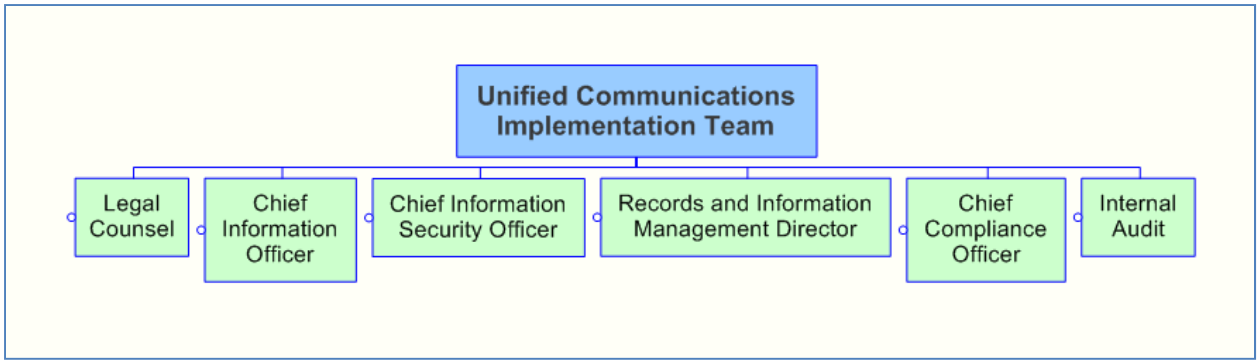
Table of Contents

Navigating compliance and security for UC solutions and services requires a commitment within the enterprise to a team-oriented approach. This Practice Toolkit provides legal counsel (whether in-house or outside), particularly those with limited familiarity with Internet security services or UC solutions or services, checklists with which to contribute to the implementation process with greater confidence and impact. These materials are not a complete "turnkey" package, but several assets are included that should allow counsel to respond directly to the analysis, and the strategies, in this Report.

As a result, some companies are better than others in their ability to work across the different management "silos" (such as Legal, IT, Security, Records Management and Compliance) and cohesively execute a specific project plan involving information technology solutions. For those companies, many of the elements of this Practice Toolkit may be redundant to, or unnecessary in light of, existing procedures, checklists and project management routines. These tools are not intended to displace those existing materials; however, a concise review may identify elements or refinements to existing management models that will help better assure that the UC solution implementation does not create legal risks that could otherwise be minimized or avoided.

1. Organize the Team

UC solutions will challenge organizational structures that have historically separated Internet-based network services from telecommunication services. That division will often exist across multiple functional competencies—IT, networking, security, legal, compliance and audit—with different methodologies, project planning and management processes. The customer enterprise acquiring a UC solution needs to candidly evaluate its existing structure and organize a team that brings the appropriate capabilities together.



While the titles, management responsibilities and organization charts vary with each organization, the required capabilities are easy to recognize. Counsel should take a special interest in assuring that the following capabilities are accounted for somewhere in the team that is organized (for the legal function, a high-level task list is also included below to highlight different skill sets that may be required):

- Legal Counsel
    - Research and report on compliance duties and requirements applicable to the types of communications and records to be created and managed by the UC solution, as well as the potential Internet security services to be employed (a checklist appears in Section 2.1 below).
    - Review existing policies and procedures to identify potential gaps, modifications or new topics to be addressed (a checklist appears in Section 2.2 below).
    - Review all existing service agreements (telecommunications, messaging, web-based communications, etc.) to evaluate cancellation, termination, transition or modification issues to consider. Vendors will often employ broadly-worded descriptions of Internet services in "first-refusal" or exclusivity arrangements that can become problematic when introducing new services.
    - Review all project plan specifications, quality of service measurement criteria and related management documentation. Counsel should work to confirm that the Security, Compliance and Audit functions within the organization are able to extract from the management documentation meaningful criteria against which to measure the functional effectiveness of the UC solutions, as well as the effectiveness of the Internet security services to be employed.
    - Prepare and/or review the RFP or similar documents to confirm the treatment of Internet security services, records management and related topics. Security and records topics are often overlooked in early stages of a project of this nature, and later attention on them can put stress on the pricing, services and overall success of any vendor contracts involved.

- Prepare, negotiate and finalize all of the related hardware, software, service, and other commercial agreements (a checklist of suggested topics appears in Section 2.3 below). Emphasis on the acceptance criteria is especially important in order to assure that the UC solutions function with the planned Internet security services and support the protection and operational management objectives.

- Chief Information Officer (CIO)
  - The Office of the CIO will provide:
    - Enterprise architecture design and management
    - IT asset inventory
    - Project management/change control management
    - Vendor management services
  - The CIO may separate Internet/Network services and telecommunication services in current management structures. Of course, UC solutions challenge those models and counsel will want to assure the right stakeholders are involved.

- Chief Information Security Officer/Chief Information Assurance Officer (CISO)
  - The CISO should be closely involved with each phase of implementing UC solutions, and work closely with counsel in defining and documenting:
    - the Internet security services to be deployed.
    - the types of monitoring, interception, access, disclosure or use activities that are contemplated.
    - the metrics to be used in real-time and retrospective management, in order to evaluate the effectiveness of the Internet security services.
    - the types of records and other operating data that will be created, and the planned management and disposition of the data.

- Records and Information Management (RIM)
  - The RIM team should help to define and classify the various temporary and long-term records to be created by the UC solutions and, for each, establish the management and disposition practices.
    - This is particularly useful for any recordings of aural transfers or other human voice activity; any long-term storage of those records should be managed against disciplined processes that protect the recordings from unauthorized

access or disclosure that may be outside the "safe harbor" discussed in Part IV—The Legal Analysis.

- Compliance and Audit
    - The compliance and internal audit functions are organized differently in various industries. However organized, both have useful roles for assuring that legal counsel's efforts to implement both compliance and security for UC solutions are properly implemented and consistently enforced.
    - Compliance and audit are particularly valuable in:
        - Confirming the legal regulations applicable to the operating records and other data assets created by the UC solutions.
        - Aligning the UC solutions with pre-existing compliance obligations (particularly those relating to specific record types (such as security brokerage customer communications) and protection of personal information or personal communications (EU or corporate privacy requirements).

2. Project Checklists

2.1 Compliance and Legal Duties Checklist

As early as possible in the overall UC solutions project, counsel should acquire a basic understanding of the types of services to be implemented, and the kinds of short-term and long-term records to be maintained in the ordinary course. Equipped with that understanding, the following questions will focus counsel's inquiry on some of the possible compliance and legal duties that may arise in connection with the proposed services:

- ☐ For each service or communication type (e.g., e-mail, voice mail, IM, VoIP, video), how are those services currently performed?
    - For each, what type of records are currently created?
        - How are those records classified under our records management program?
        - Are there any compliance duties currently mapped to those records? A sample list of possible compliance regulations appears below:

Type of Record	Applicable Compliance Regulations
Call records	Federal Communications Commission, Securities and Exchange Commission
Communication records	Securities and Exchange Commission; European privacy laws; consent-to-record laws
All records	Federal and State Rules of Civil Procedure

	(e-discovery)
Patient records	HIPAA
Books and records	IRS, Federal Energy Regulatory Commission
Assembly line accident videos	Workers Compensation

- Are there any audit or examination controls that evaluate whether the records are properly managed as required to meet compliance duties?
- Have the existing services been aligned to existing "litigation hold" programs, in order that any retained records can be specially preserved for possible disclosure or use in litigation or enforcement actions?

o For each, what type of new records will be created?

- How will those records be classified under our records management program?
- Are there any compliance duties that arise in connection with these new types of records?
- Do the new records, irrespective of the duration for which they may be stored, require or justify the imposition of access controls that may limit or foreclose access to specified individuals (e.g., only security forensic personnel conducting audits) and/or require special approvals for broader access to be permitted? For example:
  - Access to archived VoIP digital records may be limited to security forensics teams that may not convert the digital content to analog or otherwise enable the actual voices to be heard.
  - Access to recorded voice mail messages relied upon to create e-mail text messages may be limited only to those performing quality control audits to validate the accuracy of the translation functionality.

o For each, how will any of the records (whether new or currently created) be used during the period they are stored?

- Are there policies and procedures in place that describe those uses? Are other uses explicitly prohibited? If not, should they be explicitly prohibited?
- Do any compliance duties apply to the stored records (such as required media formats (*e.g.,* WORM—write once, read many).

 Will the company create and retain audible (i.e., analog) recordings of live oral communications enabled by the UC solutions (i.e., any call for which consent-to-record laws may be applicable)?

- Is the creation and retention of recorded conversations already performed by the company?
    - *If yes*, does the company currently employ consent-to-record mechanisms for those conversations?
    - *If no consent-to-record mechanisms are currently employed*, counsel should conduct a suitable state-by-state analysis to determine how to structure the consent aspects of the processes (e.g., customer calls, sales calls, applications over the phone) appropriately.
- *if the creation and retention of audible recorded conversations is to be newly performed*, counsel should conduct a suitable state-by-state analysis to determine how to structure the consent aspects of the processes (e.g., customer calls, sales calls, applications over the phone) appropriately.

☐ Will the company create and store *digital* recordings of live oral communications enabled by the UC solutions beyond the duration of the communication (i.e., after a VoIP call is completed)?

- *If no*, will the appropriate policies and procedures expressly prohibit the retention of those recordings? If so:
    - Do those policies and procedures include:
        - audit and control processes for assuring that the prohibited conduct is not being performed?
        - disciplinary provisions applicable in the event the prohibited conduct occurs.
    - Are existing training materials or policy notification mechanisms updated to communicate applicable information regarding the prohibited conduct?
    - Are appropriate technology controls allowing recordings to be created appropriately disabled or removed from administrative discretion?
- *If yes*, will the appropriate policies and procedures expressly address the creation and storage activities? If so:
    - Do those policies and procedures include:
        - at a high policy level, a statement that:
            - the use of security controls in connection with communications occurring through corporate networks and applications serve to

protect the rights and property of the company, its partners and employees and agents?

- the company employs and contracts for individuals to perform information security for the company that require them, within the scope of their employment, to access active and recorded records of communications? [1]

- descriptions of the permitted uses that can be made of the recorded assets (e.g., security forensic analysis of digital payloads) and expressly prohibit other uses (e.g., relying on the digital record to create an audible, analog version and listening to same)?

- job titles or descriptions of those allowed to make the permitted uses of the recorded assets, including specific references to the fact such uses and related activities are considered as a necessary incident to the services the related employees perform?

- notification that access logs will be created and reviewed to determine that only permitted uses have been made?

- the audit and control processes for assuring that any prohibited conduct is not being performed?

- disciplinary provisions applicable in the event any prohibited conduct occurs?

- Are existing training materials or policy notification mechanisms updated to communicate applicable information regarding the permitted and prohibited conduct?

- Are appropriate technology controls allowing recordings to be created appropriately configured with the permitted and prohibited conduct? Are additional controls in place to identify, report or otherwise track prohibited conduct?

[1] These policy statements are useful, of course, for supporting the use of information security services within an enterprise, whether or not UC solutions are being deployed.

2.2 Policies and Procedures Checklists

Information security management systems require a robust, comprehensive policy and procedure portfolio. Pursuant to the applicable standards of the International Standards Organization,[2] the policies and procedures serve several purposes:

- Express the senior leadership and commitment to information security, and the role of information security in protecting the rights and property of the company. Of course, those property assets include tangible assets as well as electronic data that is created, processed, stored and disposed of by the information systems.
- Establish the control architecture to be employed in information security, including the performance objectives, measurement criteria and reporting methods to be used in managing the security services.
- Describe the means by which information security incidents and events will be managed, including the corrective action and remediation plans to be employed following adverse incidents and events.
- Provide the measurement methods, reports and continuous improvement management process for responding to, and improving controls against, new or persistent security risks.

In implementing UC solutions, using Internet security services as part of an overall information security management program is an essential aspect for assuring that the UC solutions operate as intended and do not expose a company,its partners or employees – or their respective property assets– to unexpected risks.

The following checklist is illustrative of the topics for which responsive policies and procedures should be in place. By the very nature of UC solutions, the implementation may also require a review, update and synchronization among existing policies and procedures relating to services being replaced or enhanced by UC solutions, many of which are also identified below.

Information Security Policy and Procedure Topics

- Information Security Policy
    - Does the corporation have a formally approved information security policy?
    - Does the policy clearly express the business objectives for which security services are performed, including:

[2] *See* ISO/IEC 27001:2005, Information technology—Security techniques—Information security management systems—Requirements. Information on purchasing ISO standards is included in Appendix 2—Legal and IT Resource Inventory.

        - Stating the commitment of the company to protecting its property and the rights of the company, its officers, employees, agents and business partners?
        - Expressing that security services are a necessary incident to the use of computing and information technology?
        - Committing to use security services to protect the property of the company, its officers, employees, agents and business partners?
    - Does the policy emphasize that IT governance includes specific procedures to be adopted in furtherance of the policy, as well as the use of controls that are considered to further the expressed security and business objectives?
    - Does the policy identify the rights of the company in all networks, systems, devices and applications made available to employees, as well as the ownership by the company of all content created, transmitted, received or otherwise processed, accessed or stored by any employee or other authorized user for any reason? Does the policy expressly reserve to the employee, either by omission or express terms, any legal rights in any of such content?[3]

- Information Security Procedures
    - Telephone Usage
        - Do the procedures identify what represent permitted and prohibited uses of the telephone services available from the company?
        - Do the procedures describe the rights, or limits, on intercepting, recording or using normal telephone communications?
        - Do the procedures give notice of the types of call record information that can be logged, reported, or used by the company in managing information security?
        - Do the procedures reference, or express, corporate privacy policies and procedures regarding:
            - access rights and privileges regarding the call record information?
            - controls implementing those access rights and privileges?
            - measurement criteria for evaluating the effectiveness of those controls?
            - measurement, audit or compliance procedures for testing performance against those measurement criteria?

[3] See *infra.* Privacy Policies in this Part V.

- reporting procedures for communicating test results to appropriate management personnel?

- Do the procedures include any express consent of an employee to the recording by the company of any telephone conversation?

o Internet Usage

- Do the procedures identify what represent permitted and prohibited uses of the Internet access available from the company?

- Do the procedures describe the rights, or limits, on intercepting, recording or using records of Internet usage, history and activity by employees?

- Do the procedures give notice of the types of information that can be logged, reported, or used by the company in managing information security?

- Do the procedures reference, or express, corporate privacy policies and procedures regarding:

  - access rights and privileges regarding the Internet usage records?

  - controls implementing those access rights and privileges?

  - measurement criteria for evaluating the effectiveness of those controls?

  - measurement, audit or compliance procedures for testing performance against those measurement criteria?

  - reporting procedures for communicating test results to appropriate management personnel?

o VoIP

- In addition to telephone usage policies (addressed above), do specific procedures exist for the use of VoIP services (if part of any UC solutions or services being provided)?

- Do those procedures specifically recognize VoIP as an Internet-based service that is subject to the same types of security risks for which security services and controls are employed in support of other Internet-based services?

- Do the procedures describe the rights, or limits, on intercepting, recording or using records of VoIP usage, history and activity by employees?

- Do the procedures give notice of the types of information that can be logged, reported, or used by the company in managing information security?

- Do the procedures reference any express consents by employees to the recording of telephone conversations or other communications occurring through the VoIP services

- General Applications and Services

  - For each of the following applications or services, do specific procedures exist that reflect, as appropriate, the topics relevant to usage, records, rights and notice (as previously identified above for Telephone, Internet Usage and VoIP):

    - Electronic Mail
    - Instant Messaging
    - E-mail to Voice Mail
    - Voice Mail to E-mail
    - Mobile Devices
    - SMS or Text Messages
    - Remote Computing (homes or hotel kiosk services)

Privacy Policies

- Does the corporation have a policy addressing the privacy rights of employees with respect to information collected by the company relating to their employment, including information or data collected through their use of corporate property?

- Does the policy specifically address the expectations of employees relating to the privacy of their use of information technology systems, devices and services?

  - Does the policy give notice of the types of information that can be collected, monitored, intercepted or otherwise used by the company?

  - Does the policy give notice of specific types of monitoring, interception or surveillance procedures the company may employ as part of performing information security services?

2.3. Services Agreement Checklist

Implementing UC solutions or services involves acquiring by purchase, lease or license some combination of hardware, software applications or services. The services can be varied, including managed services (in which third parties access and manage UC solutions that are installed within a company's network) or hosted services (in which third parties operate the UC solutions outside a company's network on an outsourced basis).

Regardless of the precise contractual arrangements, any services agreement should be reviewed with a focused awareness on all of the issues raised in this Report. The following are selected topics or issues to be considered within the enterprise team and, as appropriate, addressed in the related agreements.

- Does the agreement require the vendor to make representations or warranties regarding the information security controls or processes employed in connection with the services? If software application code is employed, is the vendor required to certify the level of software assurance procedures employed in developing the code?

- Does the agreement specifically require the parties to mutually recognize that information security services (including Internet security services) must be performed as a necessary incident to the UC services? Does the agreement recognize such services are needed to protect the property and rights of the company, as well as its officers, employees or agents?

- Does the vendor maintain an information security management system with respect to the UC solutions or services being offered?[4]

- Does the agreement specify specific Internet security services required to be performed?

    - Does the agreement allocate responsibility for the performance of those services between the vendor and the company?

    - Are appropriate consents or authorizations expressed, allowing the security services to be performed as allocated?

    - For Internet security services to be performed by the vendor, does the agreement specify the specific controls to be employed by the vendor, and for each of such controls:

        - the measurement criteria for evaluating the effectiveness of those controls?

        - the measurement, audit or compliance procedures for testing performance against those measurement criteria?

        - the reporting procedures for communicating ongoing results to appropriate management personnel at the company?

        - the notice procedures for reporting security incidents or events relating to the UC services?

[4] As discussed in Part II—Internet Security Services, an "information security management system" has a precise meaning under ISO 27001. The Internet Security Alliance has previously published two books that provide detailed guidance on contracting for information security, including with vendors offering information security management systems. These books are listed in Appendix 2—Legal and IT Resource Inventory.

- the remediation and corrective action plans for responding to deficient or inadequate controls?

- Does the agreement specify the operating records to be maintained by the vendor? Are there specific provisions regarding the identities or roles of the vendor employees allowed to access those records?
    - Are specific procedures in place for those records to be accessible by the company, both during and after the term of the agreement?
    - Are specific retention practices specified for those records (storage, encryption, media, disposition schedule, etc.)?
- If VoIP or other "wire communication" services are employed, does the agreement specify whether any digital records will be preserved following the completion of any related communication?
    - If such records are to be retained, does the agreement address the conditions under which they may be accessed (*e.g.,* only by the customer)?
    - Does the agreement prohibit any other access to such records that would allow audible versions to be obtained?
- Will the vendor be recognized as an agent of the company, for the limited purpose of performing Internet security services that may be specified in the agreement?

Glossary of Defined Terms

This Glossary provides functional definitions of certain technology and legal terms used in this Report. It is not intended as an authoritative resource; other resources listed in Appendix 2—Legal and IT Resource Inventory should be consulted for further in depth analysis.

"Aural transfer" is, in summary, any communication for which any portion consists of the human voice The term is defined in ECPA in further detail and discussed in Part III.

"Byte" is a unit of eight bits, representing a single character in a computer memory. Bytes are a common measure for file sizes and computer memory (such as kilobytes, megabytes and gigabytes).

"CALEA" is the Communications Assistance Law Enforcement Act, as amended. The Act provided the basis for the FCC to examine the scope of various terms applicable to Internet-based communication services, as discussed in detail in Part III.

"Communications Act" is the Communications Act of 1934, as amended, which is the primary law administered by the Federal Communications Commission.

"Communications Enabled Business Processes" (or "CEBP") is a term describing the integration of communication functions into business applications and the ability of a communication session to access and engage with a business application. Further discussion of this concept appears in Part I.

"Electronic communication" is, in summary, any electronic communication that does not contain the human voice. The term is defined in ECPA in further detail and discussed in Part III and Part IV.

"Electronic Communications Privacy Act" (or "ECPA") is the federal law regulating the intercepting, recording and use of wire or electronic communications. ECPA often is referred to in a manner that includes the Stored Communications Act. The text of selected provisions of ECPA (and the Stored Communications Act) appears in Appendix 1.

"Electronic communications service" is, in summary, any service through which electronic communications are provided. The term is defined in ECPA in further detail and discussed in Part III and Part IV.

"Electronic communications system" is, in summary, a system through which electronic communication services are provided. The term is defined in ECPA in further detail and discussed in Part III and Part IV.

"Header" is the portion of a packet that conveys management information required for devices and applications to transmit, receive, route and process packets. An example of the content of a header appears in Part I.

"Information Security Management System" (or "ISMS") is a systematic approach to implementing information security that is described by ISO/IEC 27001 and related standards.

"Information service" is defined in the Communications Act. Discussion of information services in connection with UC solutions appears in Part III and Part IV.

"Instant Messaging" (or "IM") is a form of real-time communication between two or more persons based on text. IM products also allow other forms of real-time communication to be concurrently occurring, such as video exchanges, voice communications and file transfers.

"Intercept" is, in summary, any electronic monitoring or interception of a wire or electronic communication. The term is defined in ECPA in further detail and discussed in Part III.

"IPBX" is a PBX capable of routing and managing VoIP communications.

"MAC address (Media Access Control)" is the address used to identify actual hardware devices on a network. The MAC address is relied on in operating UC solutions and services.

"Oral communication" is, in summary, a spoken communication between individuals. The term is defined in ECPA in further detail and discussed in Part III and Part IV.

"Packet" is the unit into which message content is sub-divided for transport across a network. The Internet is a packet-switched network.

"Payload" is the portion of a packet that is the substantive content, such as part of a text document, aural transfer, video or image.

"POTS" is an acronym for "plain-old-telephone-service", specifically the traditional landline or "wired" telephone services. The interactions between POTS and UC solutions are discussed in Parts I and II.

"PBX" is a private branch exchange, a device used in companies to manage internal and external calls.

"Quality of service" is an important measure of communication services. For voice recordings, lost packets and jitter can cause degraded quality of service.

"Real Time Protocol" (or "RTP") is a key standard relied upon to provide UC solutions and services. This term is discussed in Part II.

"Secure Real Time Protocol" (or "SRTP") is a security standard that enhances RTP-based services. This term is discussed in Part II.

"Session Initiation Protocol (or "SIP") is a key standard relied upon to provide UC solutions and services. This term is discussed in Part II.

"SPIT" is spam over Internet Telephony, a form of unwanted commercial advertising.

"SPIM" is spam over Instant Messaging, a form of unwanted commercial advertising.

“Stored Communications Act” (or “SCA”) is the federal law regulating access and use of stored electronic communications. The SCA is often referred to as a part of ECPA. The text of selected provisions of SCA appears in Appendix 1.

“Telecommunications service” is defined in the Communications Act. Discussion of telecommunications services in connection with UC solutions appears in Part III and Part IV.

“Voice over Internet Protocol” (or “VoIP”) is a voice communication transported through the use of the Internet and packet-based messaging systems.

“Wire communication” is, in summary, any electronic communication for which a portion consists of a human voice. The term is defined in ECPA in further detail and discussed in detail in Part III and Part IV.

“Unified Communications” (or “UC”) are generally those solutions and services operated through the use of the SIP and RTP/SRTP protocols. How UC solutions work is described in Part I.

Appendix 1
The Electronic Communications Privacy Act of 1986

Editor's Note: The following text includes selected portions of the **Electronic Communications Privacy Act of 1986**, as amended (ECPA). All language has been adopted as published by the Legal Information Institute (LII) of Cornell Law School, available at http://www.law.cornell.edu/. Language of the United States Code is directly published at the Office of the Law Revision Counsel of the U.S. House of Representatives, available at http://uscode.house.gov/. As with any law, amendment and revision is a continuous process and the ECPA may have changes since the publication of the paper. It is suggested researchers rely on the publications of the Office of the Law Revision Counsel of the U.S. House of Representatives for the most up-to-date version of the ECPA.

18 USC Chapter 119
§ 2510. Definitions
As used in this chapter—
(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.[1]

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—
(a) any telephone or telegraph instrument, equipment or facility, or any component thereof,
(i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or
(ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;
(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

[1] So in original. The period probably should be a semicolon.

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses

enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) “contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) “Judge of competent jurisdiction” means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) “communication common carrier” has the meaning given that term in section 3 of the Communications Act of 1934;

(11) “aggrieved person” means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) “user” means any person or entity who—

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) “readily accessible to the general public” means, with respect to a radio communication, that such communication is not—

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) “electronic storage” means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) “aural transfer” means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) “foreign intelligence information”, for purposes of section 2517 (6) of this title, means—
(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—
(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—
(i) the national defense or the security of the United States; or
(ii) the conduct of the foreign affairs of the United States;

(20) “protected computer” has the meaning set forth in section 1030; and

(21) “computer trespasser”—
(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and
(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited
(1) Except as otherwise specifically provided in this chapter any person who—
(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—
(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511 (2)(a)(ii), 2511 (2)(b)–(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a) (i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518 (7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter—

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)

(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

(i) as otherwise authorized in section 2511 (2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)

(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)

(a)

(i) If the communication is—

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection—

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

§ 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally—

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of—

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications,

knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

§ 2513. Confiscation of wire, oral, or electronic communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to
(1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code,
(2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof,
(3) the remission or mitigation of such forfeiture,
(4) the compromise of claims, and
(5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

18 USC Chapter 121
§ 2701. Unlawful access to stored communications

(a) Offense.— Except as provided in subsection (c) of this section whoever—
(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
(2) intentionally exceeds an authorization to access that facility;
and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment.— The punishment for an offense under subsection (a) of this section is—
(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—
(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and
(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and
(2) in any other case—
(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions.— Subsection (a) of this section does not apply with respect to conduct authorized—
(1) by the person or entity providing a wire or electronic communications service;
(2) by a user of that service with respect to a communication of or intended for that user; or
(3) in section 2703, 2704 or 2518 of this title.

§ 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.— Except as provided in subsection (b) or (c)—
(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.— A provider described in subsection (a) may divulge the contents of a communication—
(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
(2) as otherwise authorized in section 2517, 2511 (2)(a), or 2703 of this title;
(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);
(7) to a law enforcement agency—
(A) if the contents—
(i) were inadvertently obtained by the service provider; and
(ii) appear to pertain to the commission of a crime; or
[(B) Repealed. Pub. L. 108–21, title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]
(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for Disclosure of Customer Records.— A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or

(6) to any person other than a governmental entity.

(d) Reporting of Emergency Disclosures.— On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

Appendix 2
Legal and IT Resource Inventory

This Inventory organizes the primary sources that were consulted in developing this Report. In doing so, we have attempted to list those materials that will be particularly useful to lawyers and technologists wishing to conduct more in-depth research or independently validate the analyses included.

Understanding Unified Communications

General Knowledge Resources

Baylor University Medical Center Case Study (on Unified Communications), available at http://www.cwhonors.org/viewCaseStudy2008.asp?NominationID=973 (last visited Feb. 14, 2009).

Duffy, "Enterprises Baffled by Unified Communications, Survey Says", CIO.com (June 17, 2008), available at http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Networking+and+Internet&articleId=9098798&taxonomyId=16&pageNumber=1 (last visited Feb. 12, 2009).

Edwards, "How to Get the Most from Unified Communications", CIO.com (February 8, 2008), available at http://www.cio.com/article/181550/How_to_Get_the_Most_From_Unified_Communications (last visited Feb. 12, 2009).

Grigonis, "Year-End Review and Future Trends in UC", November 18, 2008, available at http://hdvoice.tmcnet.com/topics/unified-communications/articles/45576-year-end-review-future-trends-uc.htm (last visited February 12, 2009).

Haskin, "The Brave but Speculative New World of Unified Communications", Computerworld (May 23, 2007), available at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9020921 (last visited February 12, 2009).

International Engineering Consortium, Unified Communications White Paper, available at http://www.iec.org/online/tutorials/unified_comm/index.html (last visited April 23, 2009).

Linask, "Network Security in the Face of Growing Threats", April 16, 2009, available at http://small-business-voip.tmcnet.com/topics/smb-voip/articles/54420-network-security-the-face-growing-threats.htm (last visited April 22, 2009).

Parker, "Top UC Applications are Now Apparent", Business Communications Review (June 2007), available at, http://www.unicommconsulting.com/library/BCR_June_2007_UC_Applications.pdf (last visited February 7, 2009).

Vendor/Supplier Websites

The following websites published by vendors or suppliers of UC products or services are representative of those visited in conducting the research for this paper; these websites provided product descriptions, market analyses and, in several instances, published materials discussing legal and regulatory aspects considered with respect to their products or services. The listing of these vendors is not intended to endorse their products, nor the views expressed on their websites (the vendors are listed in alphabetical order):

Anagran, www.anagran.com

Avaya, www.avaya.com

Facetime, www.facetime.com/default.apx

Microsoft Corporation, www.microsoft.com/uc/what.mspx

Mobile in a Minute, www.mobilein.com/unified_messaging.htm

Nortel Communications, www.nortel.com

Quintum Technologies, www.quintum.com

Salare Security, www.salaresecurity.com

SKC Communications, www.skccom.com

Skype, www.skype.com

Symantec, www.symantec.com

Vonage, www.vonage.com

http://www.sipcenter.com/

Industry Publications and Websites

The following general industry publications and websites focusing on unified communications products and services are representative of those visited in conducting the research for this paper; the listing of these publications and websites is not intended to endorse their products, nor the views expressed on their websites (the publications and websites are listed in alphabetical order):

CIO.com, www.cio.com.

Search Unified Communications, http://searchunifiedcommunications.techtarget.com/#.

> Research included numerous white papers and other publications in the Unified Communications Research Library available on this website.

SIP Center, www.sipcenter.com.

Described as a portal for commercial SIP development.

TMC.net, www.tmc.net.

Includes online content of Unified Communications Magazine.

Voice Over IP Security Alliance (VOIPSA), www.voipsa.org.

VoiP News, www.voip-news.com

VoIP Info, http://www.voip-info.org

Information Security

The information security field is highly technical and sophisticated knowledge resources exist on a large variety of topics addressed in this Report. The following resources address information security and include special attention to related legal issues

Bosworth, Kabay & Whyne, Computer Security Handbook,5th Edition (John Wiley & Sons, Incorporated) (2009).

Internet Engineering Task Force (www.ietf.org).

Publishes various standards relating to Internet services, including those relied on for unified communications.

Internet Security Alliance (www.isalliance.org)

Contracting for Information Security in Commercial Transactions, Volume I: An Introductory Guide

Contracting for Information Security in Commercial Transactions, Volume II: Model Contract Terms for Certified Information Management Systems

The following organizations offer significant resources and information:

Information Systems Security Association, www.issa.org.

ISACA, www.isaca.org.

ITIL, www.itil-officialsite.com.

Standards referenced in this Report may be purchased from www.iso.org as well as national standards organizations (such as the American National Standards Institute, www.ansi.org).

Legal Resources

General Legal Information

The following websites include useful general information regarding ECPA and related topics:

Center for Democracy and Technology, www.cdt.org. CDT has published a variety of studies and papers on different legal aspects of information technology, with a focus on privacy.

Cybertelecom, Federal Internet Law & Policy, An Educational Project, available at http://www.cybertelecom.org/security/ecparef.htm (Last visited May 10, 2009).

Articles

The following articles are useful starting points for various key topics covered in this Report:

Bucci, "Call Recording and the Law: A Comprehensive Guide to Compliance and Best Practices", available at http://www.tmcnet.com/tmc/library/librarydownload.aspx?id=712&type=1&title=Call+Recording+and+the+Law+A+Comprehensive+Guide+to+Compliance+and+Best+PracticesCall+Recording+and+the+Law+-+A+Comprehensive+Guide+to+Compliance+and+Best+Practices (last visited Feb. 12, 2009).

Burnside, "The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Communication Technologies, 13 Rutgers Computer & Tech. L. J. 451 (1987).

Crawford, "CALEA 2005-2007 Roundup", available at http://scrawford.blogware.com/blog/archives/2007/8/16/3162684.html (last visited Feb. 10, 2009).

Dempsey, "Digital Search and Seizure: Updating Privacy Protections to Keep Pace With Technology", 902 PLI/ PAT 407. Practising Law Institute. June-July 2007. (last visited February 17, 2009).

Greenberg, "E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute," 44 Am. U. L. Rev. 219 (1994) ("Note").

Kerr, "A User's Guide to the Stored Communications Act, and a legislator's guide to amending it", 72 Geo. Wash. L. Rev. 1208 (2004).

Kiser, "VoIP Services Regulation 2008: Tracking the Evolving Regulatory Framework" 925 PLI/Pat 15. Practising Law Institute. January-March 2008. (last visited on February 12, 2009).

Mulligan, "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557 (2004) ("Mulligan").

Oza, Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty, 88 B.U.L.R. 1043 (October 2008) (last visited February 20, 2009)("Oza").

"The ECPA, ISPs and Obtaining E-Mail: A Primer for Local Prosecutors", (National District Attorneys Association, at http://www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf.

Smedinghoff and Hamady, "New Data Security Regulations Create Compliance Challenges for Businesses," The Secure Times (Vol.4, No.1, 2009), at 2. Available at http://privacylaw.wildman.com/article/Secure_Times_Winter_2009.pdf

Laws and Regulations

The following are relevant laws and regulations to be considered from a compliance perspective in implementing any unified communications solutions or services:

United States Federal Laws and Regulations

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 2001 HR 3162, enacted October 26, 2001.

Communications Act of 1934, Pub. L. No. 416, 48 Stat. 1064, enacted June 19, 1934.

Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010, enacted in 1994.

Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2008).

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, enacted October 21, 1986.

Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338, enacted November 12, 1999.

Health Insurance Portability and Accountability Act of 1996, Pub. L. No.104-191, Administrative Simplification Sec 261-262, Sec 1171-1179, enacted August 21, 1996.

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, enacted July 30, 2002.

17 CRF 240.17a-4 (Securities and Exchange Commission regulations on brokerage customer communications and records) .

DOD Standard 5015.2-STD, Electronic Records Management Software Applications Design Criteria Standard (2007).

Fed. R. Civ. P. 26, Duty to Disclose; General Provisions Governing Discovery.

ECPA Legislative History References

Electronic Communications Act of 1986, S. Rep. 99-541, 1986 U.S.C.C.A.N. 3555.

Electronic Communications Act of 1986, H. Rep. 99-647.

FCC Orders, Decisions and Related Case Law

The Federal Communications Commission has given extensive attention to how Internet-based communications and services are to be considered under the Communications Act and related laws. Here is a starting list of the relevant orders, decisions and case law:

FCC 05-153, First Report and Order and Further Notice of Proposed Rulemaking, Adopted: August 5, 2005 Released: September 23, 2005. 20 FCC Rcd. 14989 (Sept. 23, 2005).

Cable Modem Ruling- Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, GN Docket No. 00-185, Declaratory Ruling and Notice of Proposed Rulemaking, 17 FCC Rcd. 4798 (2002) ("Cable Modem Ruling").

Wireline Broadband Order- Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, CC Docket No. 02-33, Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd. 14853 (2005) ("Wireline Broadband Order"), *aff'd,* Time Warner Telecom, Inc. v. FCC, 507 F.3d 205, WL 2993044 (3d Cir. Oct. 16, 2007).

Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket 04-295, First Report and Order and Further NPRM, 20 FCC Rcd. 14989 (Sept. 23, 2005) ("*CALEA Broadband Order*"). The FCC had defined "facilities-based" providers as those entities that "provide transmission or switching over their own facilities between the end user and the Internet Service Provider (ISP)."

Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295, Second Report and Order an Memorandum Opinion and Order, 21 FCC Rcd. 5360 (2006) ("*CALEA Second Order*").

In the Matters of IP-Enabled Services Implementation of Sections 255 and 251 (A)(2) of the Communications Act of 1934, as enacted by the Telecommunications Act of 1996: Access to Telecommunications Service, Telecommunications Equipment and Customer Premises Equipment by Persons with Disabilities, 22 FCC Rcd. 11275, ¶ 21 (2007) ("*VoIP Disability Access Order* ").

American Council on Education v. F.C.C., 451 F.3d 226 (DC, June 9, 2006). Available at http://pacer.cadc.uscourts.gov/docs/common/opinions/200606/05-1404a.pdf (last visited Feb. 10, 2009).

AT&T v. City of Portland, 216 F.3d 871 (9th Cir. 2000).

Brand X Internet Servs. v. F.C.C., 345 F.3d 1120 (9th Cir. 2003).

Chevron USA Inc. v. NRDC, 467 U.S. 837, 843-844 (1984).

ECPA and Related State Case Law

Most of the following cases have been cited in this Report; however several of them are also included here to provide a more complete listing of the key decisions interpreting ECPA and related state laws.

Fraser v. Nationwide Mut. Ins. Co., 135 F.Supp.2d 623, (E.D.Pa.,2001) (interception only occurs during the transmission process).

Griggs-Ryan v. Smith, 904 F.2d 112 (C.A.1 (Me.), 1990) (implied consent dealing with telephone converstions).

Jayne v. Sprint PCS, Slip Copy, 2009 WL 426117 (E.D.Cal., 2009).

Kearney v. Salomon Smith Barney, 39 Cal.4th 95, 137 P.3d 914 (Cal.,2006) (proof of notice, this dealt with consent to record).

Hause v. Commonwealth, 83 S.W.3d 1, 11-12 (Ky.Ct.App.2001).

In re Forgione, 49 Conn. Supp. 613, 908 A.2d 593, 607-08 (Super.Ct.2006).

In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 497 (S.D.N.Y. 2001) (email messages stored on an ISP awaiting delivery were in "temporary, intermediate storage").

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002) (held that "intercept" applies to "acquisition contemporaneous with transmission").

Morano v. Slattery Skanska, Inc., 846 N.Y.S.2d 881 (N. Y. Sup. Nov 28, 2007) (cell phone call records).

Quon et al. v. Arch Wireless Operating Co. Inc., No. 07-55282, 2008 U.S. App. LEXIS 12766 (9th Cir. Jun. 18, 2008) (city violated privacy rights by reading text messages).

Smith v Maryland, 442 US 735 (1979).

Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994) (messages stored on a bulletin board service pending delivery were in "temporary, intermediate storage").

Theofel v. Farey-Jones, 359 F.3d 1066 (C.A.9, 2004) (messages after delivery continued to be stored on ECS server were stored "for purposes of backup protection" within the ordinary meaning of those terms).

United States v. Forrester, 512 F.3d 500 (Cal. 2008) (e-mail and Internet users have no expectation of privacy in to/from transmittal data or IP addresses).

United States v. Reyes, 922 F.Supp. 818, 836 (S.D.N.Y.1996) ("the acquisition of the data [must] be simultaneous with the original transmission of the data").

Appendix 3

Research Notes

Preparing this Report required research into both technology and the law. The research was made challenging by the concurrent real-time realities:

- Functionally, unified communications solutions are dynamic and subject to rapid innovation and integration as vendors continue to refine and focus their product offerings to meet the fast-changing needs of the market. This Report was prepared during economically challenging times and, as a result, the vendors and their customers were constantly adjusting to the challenges.

- In addition, the Federal government, led by a new Administration in early 2009, placed a priority on cybersecurity, while the headlines continued to announce new system vulnerabilities, successful attacks and compromised networks and software applications. Concurrent to the preparation of this Report, the Administration was conducting an extensive review of the nation's cybersecurity, and our responsive resources, policies and practices and legal framework.

While these factors did not influence the outcome of our research, they may put at risk the long-term utility of our analysis. Those reviewing the Report are strongly encouraged to consult appropriately qualified legal and technology professionals to confirm the continued validity of our analysis.

Understanding Unified Communications

To confirm our understanding of the unified communications and the related Internet security service issues, as well as how industry was viewing those issues, we completed the following activities:

- Searching the Internet, we identified and reviewed:
    - general industry-focused websites, focusing on UC solutions and services.
    - over 20 different vendor websites, on which we reviewed:
        - products and service descriptions, including technical specifications.
        - vendor-generated white papers on implementation topics, including regulatory compliance. (Notably, none discussed ECPA or related compliance topics, focusing instead on records retention rules under varied Federal regulations (e.g., health information, securities brokerage customer communications, financial services, etc.).

- specific websites on Internet security services relating to UC solutions (such as www.voipsa.org) and their substantive papers, materials and discussion forums.

- Conducted in-depth product and service discussions with several major vendors of UC products and services (all discussions were held on a confidential basis). These discussions allowed us to also gain access to understanding the vendor's perspective on the legal and compliance issues to which we were giving attention.

- Attended multiple sessions of the SCAP standards project of the Internet Security Alliance (discussed in the Introduction) and reviewed their work papers and products to identify and understand the project scope and issues. We also conducted extended discussions with participants in the SCAP project to confirm our understanding of the technologies and related security services.

- Interviewed corporate security officers and teams from Internet Security Alliance member companies, and their executives, to document their concerns on legal and compliance issues and validate that our research was properly focused on the types of UC services, and Internet security services, in which the member companies were interested.

- During the research, Waters Edge also participated concurrently in the development and launch of the Cloud Security Alliance, a new non-profit organization promoting the use of best practices for providing security assurance within cloud computing (Internet-based services), and the guidance documents authored by their advisory group.

Understanding the Law

While there is a growing body of law that might be classified as information security law, or cyber law, we recognized early in our research that there were few direct precedents relating to the legal aspects of the security services to be applied to UC communications. Therefore, our research dug deeply into the legislative history of the key laws (ECPA as well as the Communications Act) as well as a detailed review of relevant law review articles and, of course, judicial case law.

Our research was conducted through Westlaw as the primary research vehicle, as well as reliance on law review articles and other secondary sources to direct us to other relevant legal materials. The substantive materials are listed in the Legal and IT Resource Inventory.

The technical integrity of our legal analysis (i.e., were we correctly applying the law to the relevant technology features and services) was confirmed through interviews and reviews with those corporate representatives previously interviewed. As well, interviews with other authorities in the law of privacy and information security served to confirm the focus and direction of our research and our analysis.