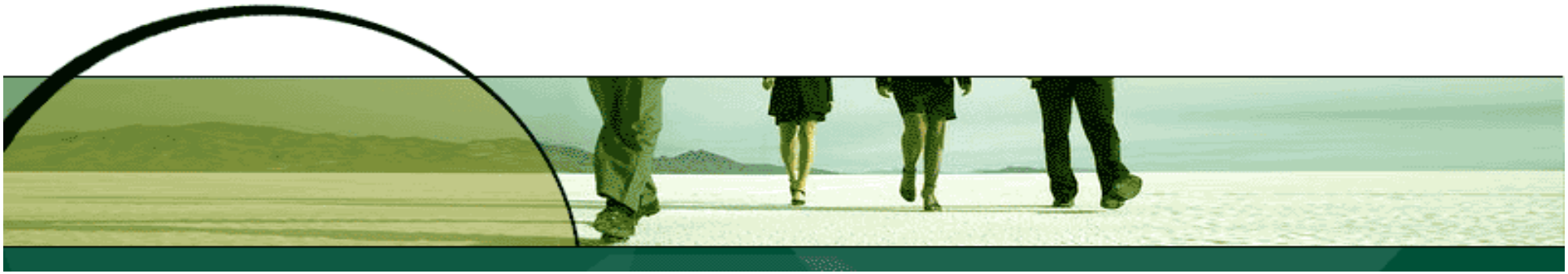
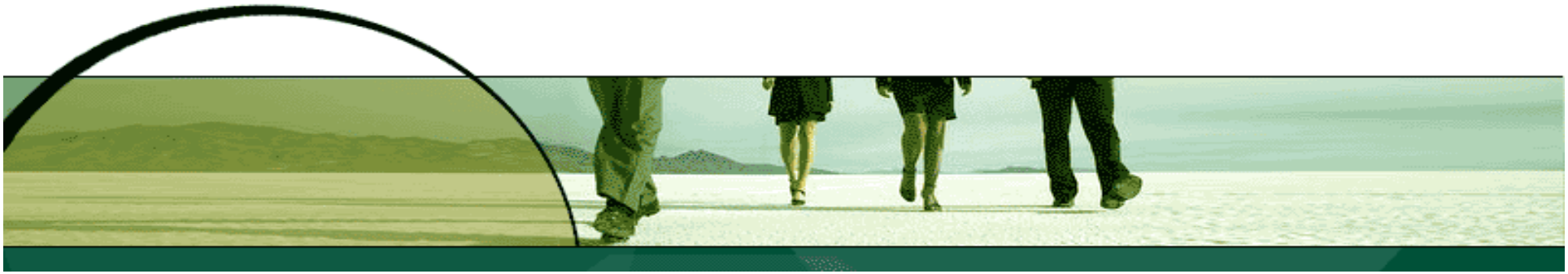
The Impact of Changing Regulations and Technology on an Organization's Privacy and Data Protection Policies

K.C. Halm, Davis Wright Tremaine, LLP
Greg Kopta, Davis Wright Tremaine, LLP
Heidi Salow, DLA Piper, LLP



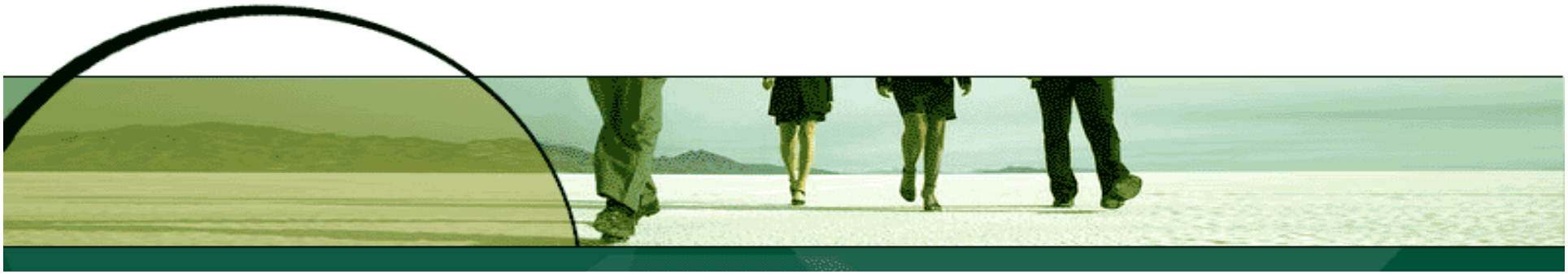
Overview:

- Part 1 – Surveillance of Communications Networks and Services
- Part 2 – Pretexting and Telephone Records Privacy
- Part 3 – Privacy Restrictions Affecting Commerce Over Communications Networks
- Part 4 – A Look Ahead



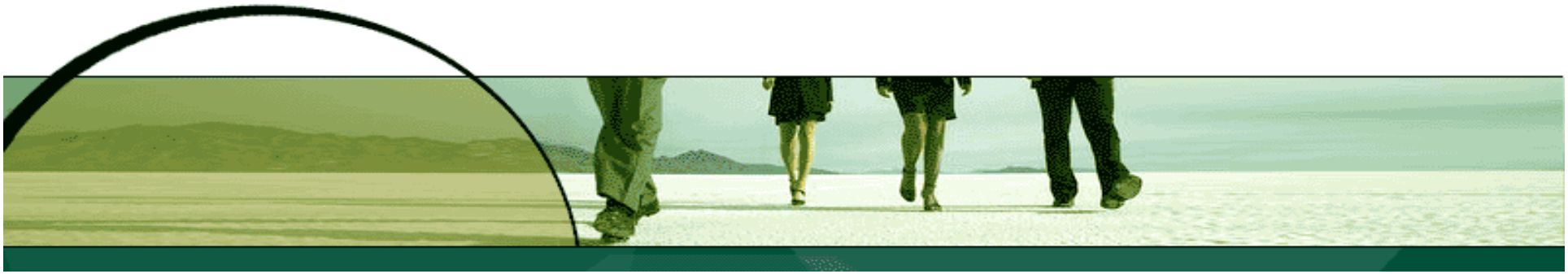
Part 1

Surveillance of Communications Networks and Services



Surveillance of Communications Networks and Services

- Background and basics
  - Authorized interception of electronic communications and voice transmission signals
  - Governed by multiple legal authorities
    - Fourth Amendment
    - Wiretap Act, Pen Register/Trap & Trace Statute, Electronic Communications Privacy Act, the Cable Act, and FISA
  - Subject to various levels of government search authority
    - Court orders, warrants, subpoenas

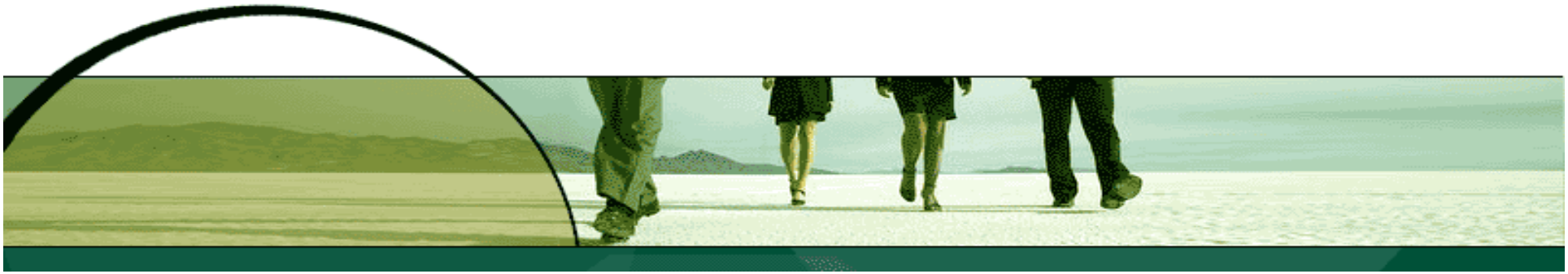


Wiretap/Surveillance Activities

- Must provide “information, facilities, or technical assistance” to persons authorized by law to intercept wire, oral, or electronic communications if so directed by court order.
- Normally obtained pursuant to court order, where judge finds probable cause of likelihood of the commission of certain felony offenses.
- Notice Prohibited
  - Notice to subscriber of existence of surveillance or intercept device is prohibited, unless “otherwise required by legal process,” and then only after prior notice to the Attorney General or principal prosecuting attorney of applicable jurisdiction.

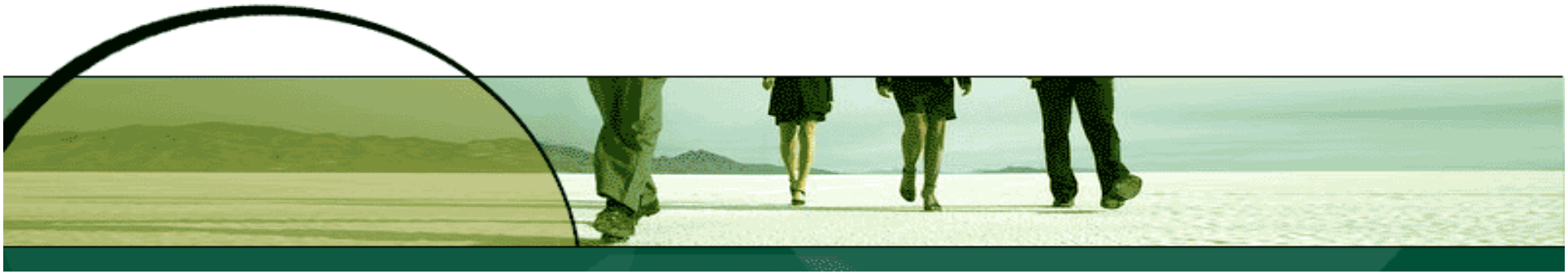
Pen Register/Trap & Trace Activities

- Furnish law enforcement with “all information, facilities, and technical assistance” necessary to accomplish installation of pen register or trap and trace device, if directed by court order.
- Emergency installations (without court order, allowed under certain circumstances).
- Results of trap and trace device must be provided to the law enforcement agent at regular intervals.
- Law enforcement agencies may, by Federal or State court order, and without notice to you, obtain the right to install a device that monitors the addressing and routing of your Internet and electronic mail use, but not the contents of your electronic mail.



Foreign Intelligence Surveillance Act - FISA

- Regulates conduct of “electronic surveillance” and “physical search” for foreign intelligence / law enforcement purposes.
- Amended after Sept. 11 to enhance law enforcement and intelligence gathering against international terror targets.
- FISA-authorized surveillance acts are issued by secretive “Foreign Intelligence Surveillance Court.”

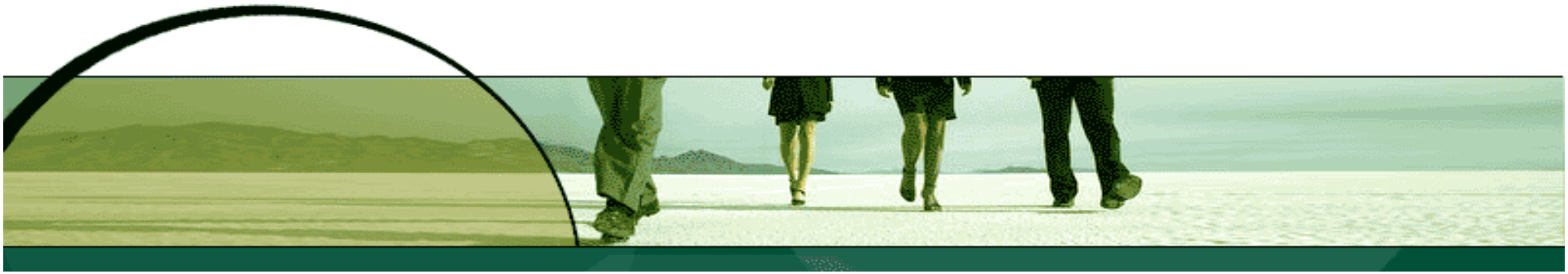


FISA Controversy: *NSA Surveillance Litigation*

- Following 9/11 attacks President secretly authorizes National Security Agency to initiate a program of warrantless electronic surveillance within the U.S.
- Existence denied for several years, but Administration publicly acknowledged the program following *New York Times* report in December 2005.
- Since then, government officials have explained the nature and scope of the Program as involving the interception, inside the United States, of both e-mail and telephone communications

FISA Controversy: *NSA Surveillance Litigation*

- Federal District Court: Program violates the 4th Amendment; 1st Amendment free speech rights; and was not authorized by authorization of military force following 9/11 attacks.
- US Court of Appeals for the Sixth Circuit: District court decision reversed for lack of "standing"; and failure to demonstrate that the plaintiffs communications had been monitored by the NSA program.
- Congress enacts the Protect America Act ("PAA").
  - PAA allows government to conduct warrantless electronic surveillance if the surveillance is "directed at" or "concerns" someone reasonably believed to be outside the United States.
  - FISA Court's role is limited to reviewing reasonableness of procedures used by the executive to determine whether individuals are outside the United States.



Surveillance of VoIP and Broadband ISP Networks - CALEA

- Authorized surveillance pursuant to federal statute known as CALEA (Communications Assistance for Law Enforcement Act).
  - FCC recently expanded reach of CALEA beyond traditional telecommunications carriers to “interconnected Voice over Internet Protocol” (“VoIP”) providers and facilities-based broadband ISPs.
  - VoIP providers and broadband ISPs must modify and design their network to have capabilities necessary to allow government electronic surveillance.
- *Unauthorized* surveillance activities are also a consideration.

Surveillance of VoIP and Broadband ISP Networks - CALEA

- Network modifications and assistance capabilities mandated by May 14, 2007.
- Affected providers must be able to respond to law enforcement surveillance requests by expeditiously isolating and enabling:
  - interception of all wireline and electronic communication; and
  - access to “call-identifying” information, and call content, reasonably available to the carrier.

Surveillance of “Electronic Communications” - ECPA

- ECPA is an amendment to, and extension of, the original Wiretap Act
- Amended existing statute to include the interception of electronic communications, which include wireless and wired transmissions, including electronic mail.
- ECPA also extended protections to “stored” communications by prohibiting the unauthorized access to information in electronic storage, i.e. content of e-mail and voice messages, and personally identifiable information pertaining thereto.

Surveillance of "Electronic Communications" - ECPA

- Upon receipt of a Federal or State search warrant or court order service provider must disclose to government (law enforcement) without advance notice to the subscriber:
  - Web surfing records/ IP address confirmations from logs
  - All e-mails (subject to 6th Circuit's recent "Warshak" decision)
  - Not video choices if cable service subscriber
  - Emergencies and NCMEC (child abuse) reports
  - Billing/Payment Records

"DECISION TREE" / MATRIX FOR RESPONDING TO GOV'T REQUESTS FOR SUBSCRIBER INFO

Red = Cable Only Subscribers
Blue = Internet Subscribers
Green = Telephony Only Subscribers

Administrative, Grand Jury or Trial **Subpoena** from Government Entity

OR

Search Warrant from Government Entity

OR

Court Order Disclosure to Government Entity

OR

VOLUNTARY DISCLOSURE to Government Entity

NOTE
FOR DISCLOSURES to Non-Government Entities (voluntary and non-voluntary)

Cable Subscriber Only
Cable Act Controls

Must disclose personally identifiable subscriber information to a governmental entity, including viewing habits, pursuant to a court order only if, in the court proceeding relevant to such court order,

- the government offers clear and convincing evidence that such records are material to a criminal investigation; and
- the subscriber is given the opportunity to appear and contest the evidence presented by the government. (*i.e.*, **with advance notice** to the subscriber).

Internet Subscriber
(May also be cable subscriber)— Use ECPA

OLD CONTENT ONLY (Emails > 180 days)

Must disclose contents of a wire or electronic communication upon receipt of a court order with no advance notice of disclosure to subscriber. 18 U.S.C. § 2703(b).
DO NOT DISCLOSE content of recent communications (180 days or less) unless government receives consent from the subscriber.

MONITORING

Must allow law enforcement agencies, by court order, and without advance notice to subscriber (if so directed by gov't.), to install a device that monitors the addressing and routing of subscriber Internet and electronic mail use, but not the contents of subscriber electronic mail.

SUBSCRIBER RECORDS

Upon receipt of a court order, must disclose, without advance notice to subscriber a record or other information pertaining to a subscriber, but not including content, including:

- Subscriber name and address;
- records of subscriber Internet sessions (including session times and duration);
- how long subscriber has subscribed to our service(s) (including start date) and the type(s) of service(s) utilized;
- subscriber telephone number or other subscriber account identifying number(s), including any Internet or network address(es) (e.g., static or dynamic IP addresses) assigned to subscriber by our network; and
- the means and source of subscriber payment(s) (including any credit card or bank account number)

HOWEVER, records may not reveal subscriber selection of video programming unless court order in compliance with Cable Act requirements.

Telephony Subscriber
(May also be cable and/or Internet sub)
Use Wiretap Act and Pen Register Statute

CONTENT (No restriction on old or new)

WIRETAP/SURVEILLANCE ACTIVITIES:

Must provide "information, facilities, or technical assistance" to persons authorized by law to intercept wire, oral, or electronic communications if so directed by Court Order.

Notice to subscriber of existence of surveillance or intercept device is PROHIBITED, unless "otherwise required by legal process," and then only AFTER gives prior notice to the Attorney General or principal prosecuting attorney of applicable jurisdiction.

MONITORING

PEN REGISTER/TRAP & TRACE ACTIVITIES:

Furnish investigative or law enforcement officers with "all information, facilities, and technical assistance" necessary to accomplish installation of pen register or trap and trace device, if so directed by Court Order.

Results of trap and trace device must be provided to the law enforcement agent at regular intervals.

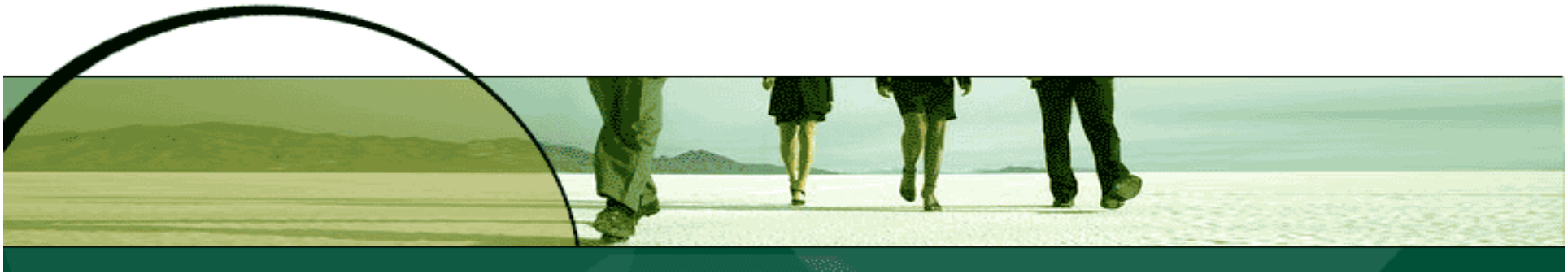
SUBSCRIBER RECORDS

CPNI (information re quantity, configuration, type, destination, location and amount of use of a telecommunications service):

has a general duty to protect subscriber privacy. However, that duty is subject to broad statutory exception that allows for disclosure of CPNI "as required by law." At least one federal court has relied upon this broad exception to compel a carrier to produce to an opposing party discovery that included CPNI. * Also obligated to provide subscriber records pursuant to court, under same circumstances as when required by warrant or subpoena.

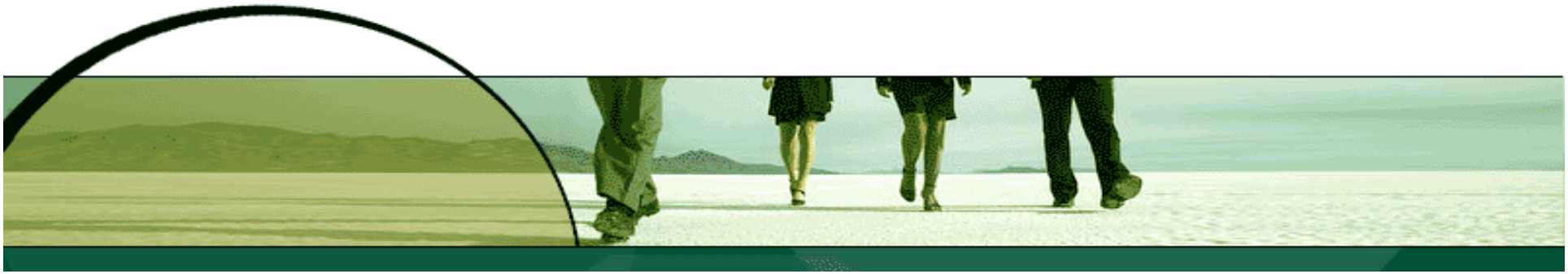
Part 2

Pretexting and Telephone Records Privacy



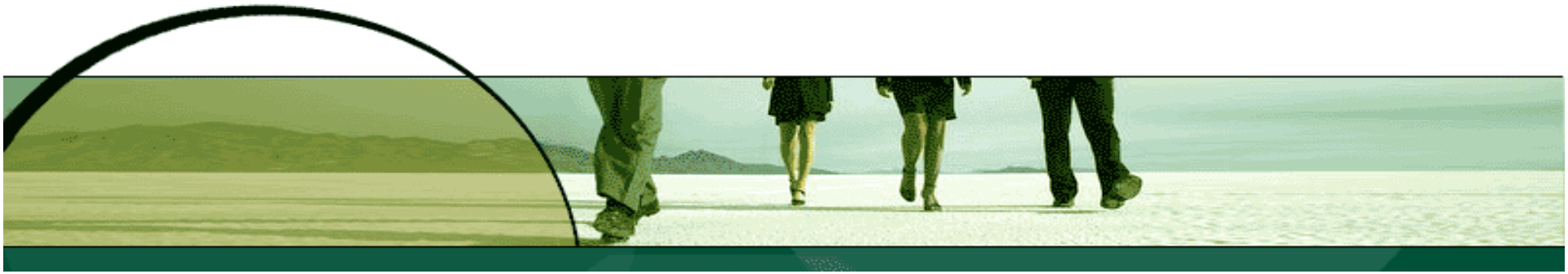
CPNI

- Customer Proprietary Network Information
  - What it is
  - What protections/restrictions apply
  - Who is restricted
  - Who is protected
  - Potential Issues



Definition of CPNI

- CPNI includes personally identifiable information derived from a customer's relationship with a provider of communications services. Examples:
  - Type and quantity of services provided
  - Details of calls made and received
  - Account history

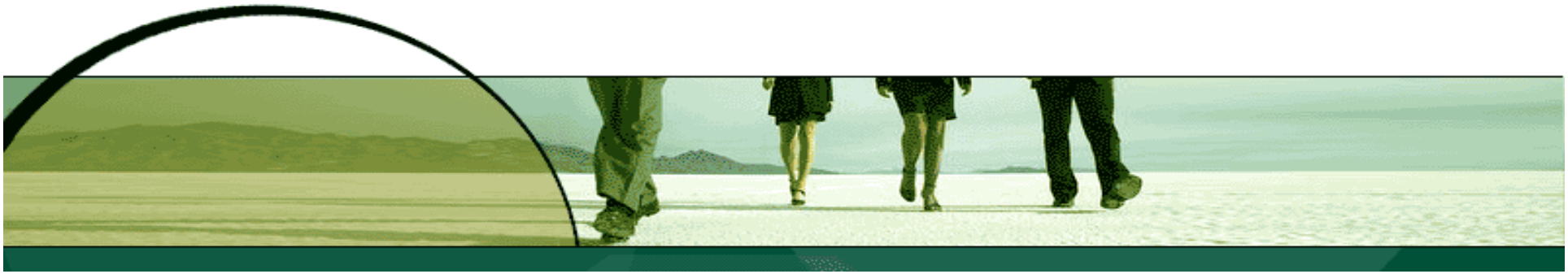


General Protections for CPNI

- A carrier may only use, disclose, or permit access to customers' CPNI:
  - As required by law;
  - With the customer's approval;
  - In the provision of service from which the information is derived or services necessary to or used in such services.
- Customers have a right to obtain access to, and compel disclosure of, their own CPNI

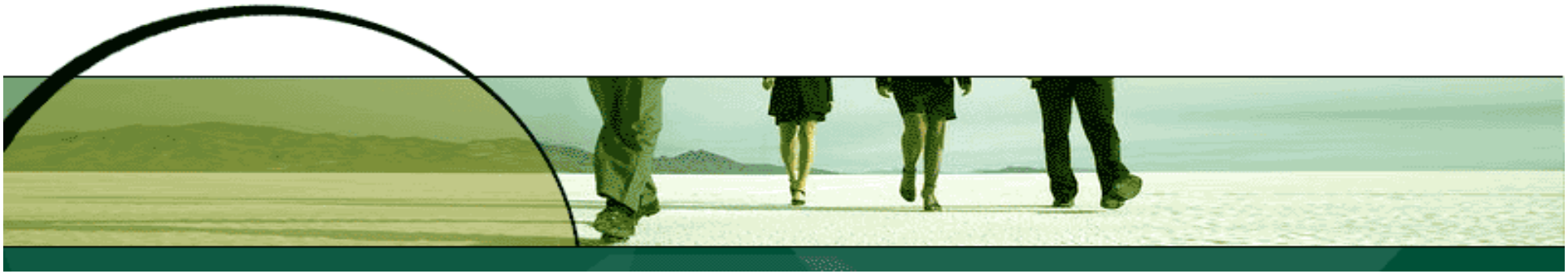
Call Detail CPNI

- "Call detail" or "call records" includes any information that pertains to the transmission of specific telephone calls, including:
  - Telephone number
  - Time, location, or duration of call
- Does not include general usage information, such as remaining minutes of use



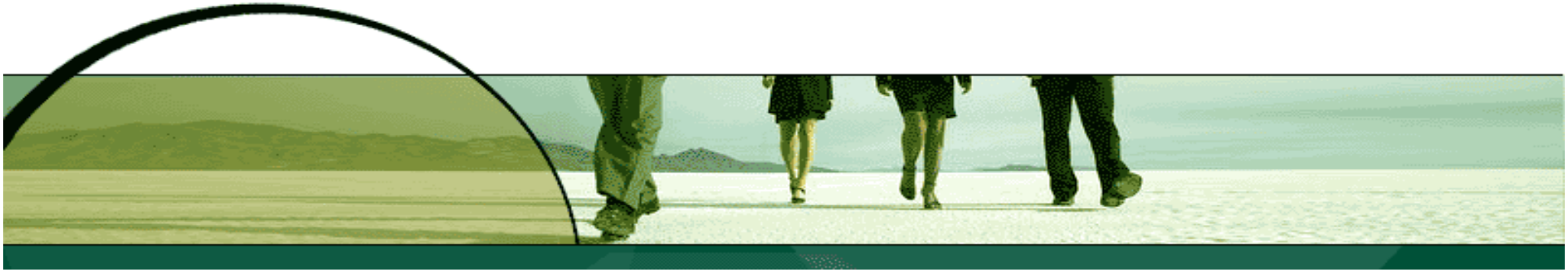
Carrier Authentication Requirements

- Carriers cannot release call detail based on customer-initiated contact except:
  - If customer provides a pre-established password
  - If the carrier sends the information to the customer's address of record
  - If the carrier calls the customer at the telephone number of record
  - For in-store contact, if customer shows valid photo ID
  - Carriers may provide customer service using call detail provided by the customer during the contact without a password if that service does not require carrier disclosure of additional call detail
- Carriers must password protect online access to all CPNI



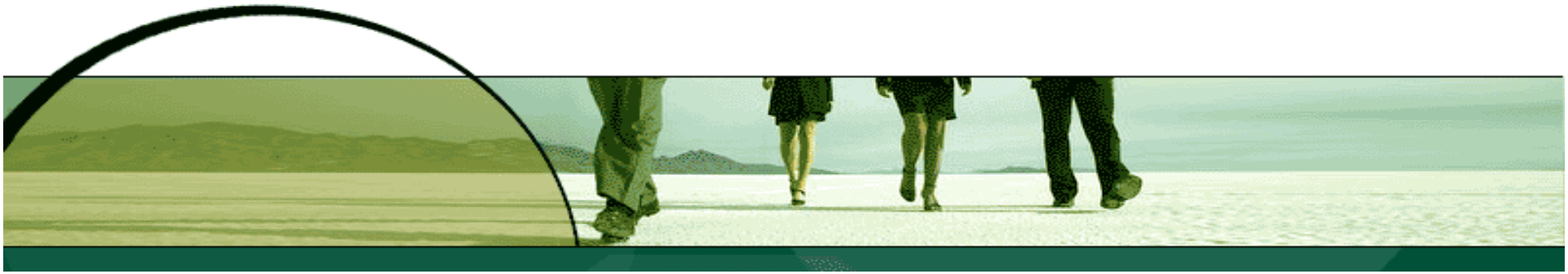
Password Protection

- Establishment of Password Protection
  - For new customers at time of service initiation
  - For existing customers after authentication without the use of readily available biographical information or account information
- Use of Password Protection
  - Carriers cannot prompt customers for passwords by asking for biographical/account information
  - Carriers may create back-up customer authentication procedure for lost or forgotten passwords not based on biographical/account information



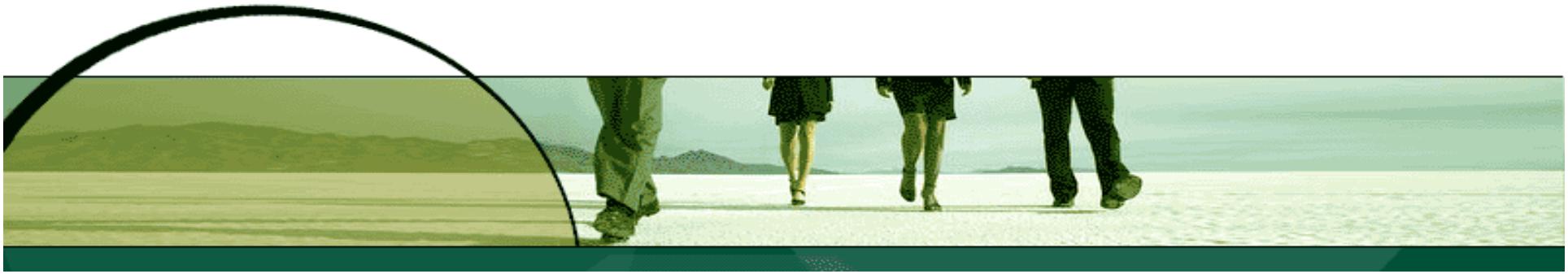
Notification Requirements

- Carriers must immediately notify customers of creation or changes to a password, customer response to a carrier-designated back-up means of authentication, online account, or address of record
- Carriers must notify law enforcement (within 7 business days) and customers (thereafter) whenever a security breach results in that customer's CPNI being disclosed to a third party without that customer's authorization



Who Must Comply

- Communications service providers
  - Landline local and long distance carriers (e.g., AT&T, Verizon, Qwest)
  - Wireless carriers (e.g., T-Mobile, Sprint-Nextel)
  - Interconnected VoIP providers (e.g., Vonage, Skype)
- NOT expressly applicable to:
  - Shared Tenant Service Providers
  - Businesses with private network or PBX
  - Non-interconnected (private) VoIP networks

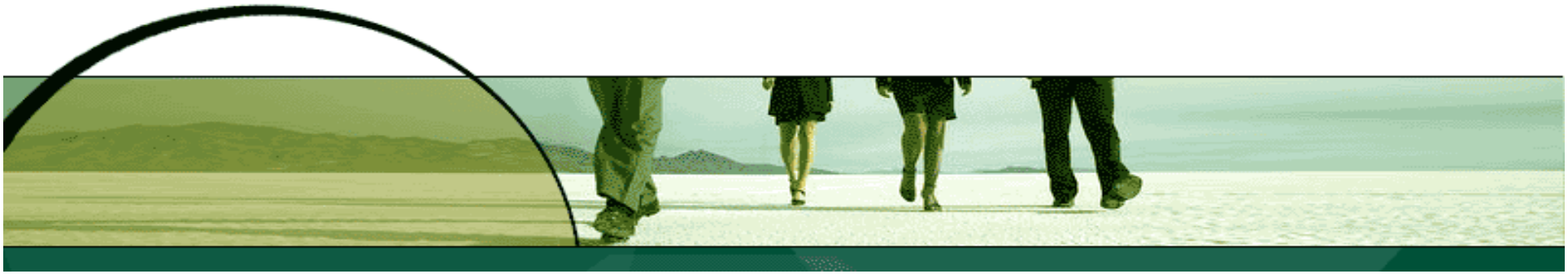


Who Is Protected

- Customers – not defined but generally accepted as the person(s) in whose name(s) the service account is maintained
- Business customer exemption – Carrier authentication and notification requirements do NOT apply to businesses that have a contract with a service provider that
  - Specifically addresses the provider's protection of CPNI; and
  - Is serviced by a dedicated account representative as the primary contact

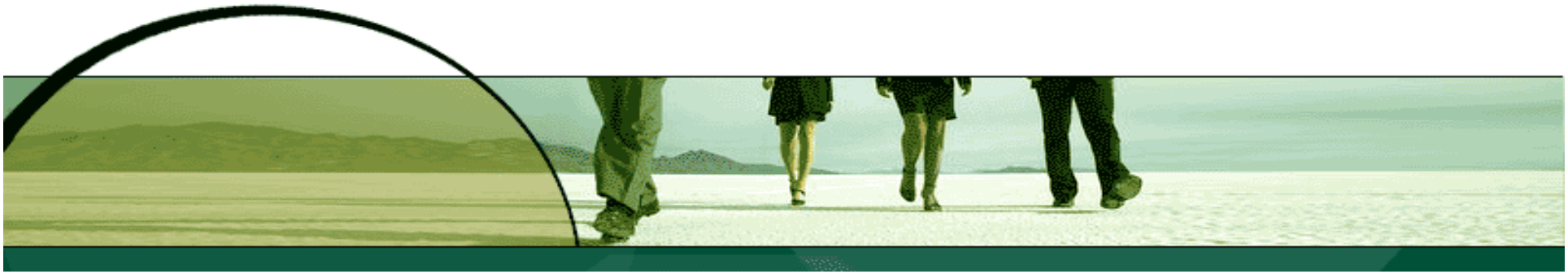
Potential Issues

- Exempt business customers – must ensure contract with service provider adequately addresses CPNI protection
- Nonexempt business customers – must establish CPNI procedures, including who within the company controls access to CPNI
- All business customers – may need to review how employees obtain service used for business purposes (i.e., through the company or independently with company reimbursement)



Part 3

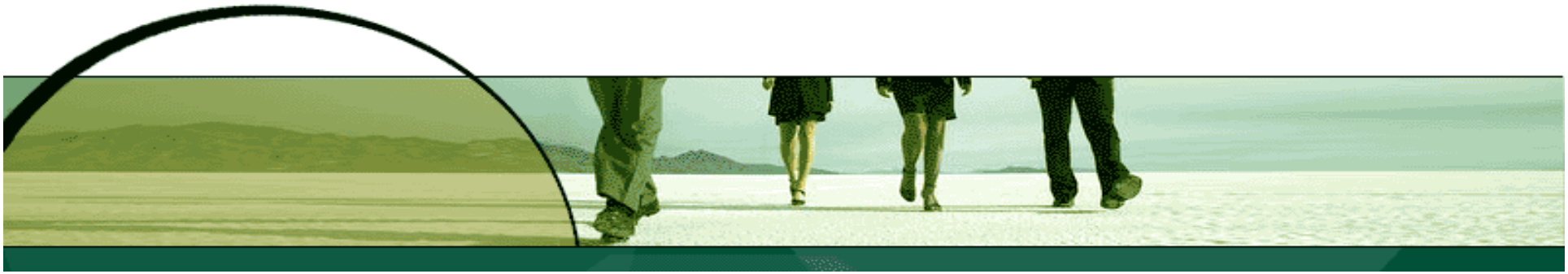
Privacy Restrictions Affecting Commerce Over Communications Networks



Email Marketing - CAN SPAM Act

What's Required?

- Indicate that email is a solicitation/commercial email message (CEM)
- Identity of sender and sender's physical address
- Convenient opt-out option for each message
- Prohibits further emailing by sender or sharing of the recipient's email address if recipient opts out
- CEMs defined to mean e-mail messages the "primary purpose" of which is the commercial advertisement or promotion of a "commercial product or service"
- Applies to both "business-to-consumer" and "business-to-business" CEMs
- Exception for emails that are "transactional or relationship" in nature



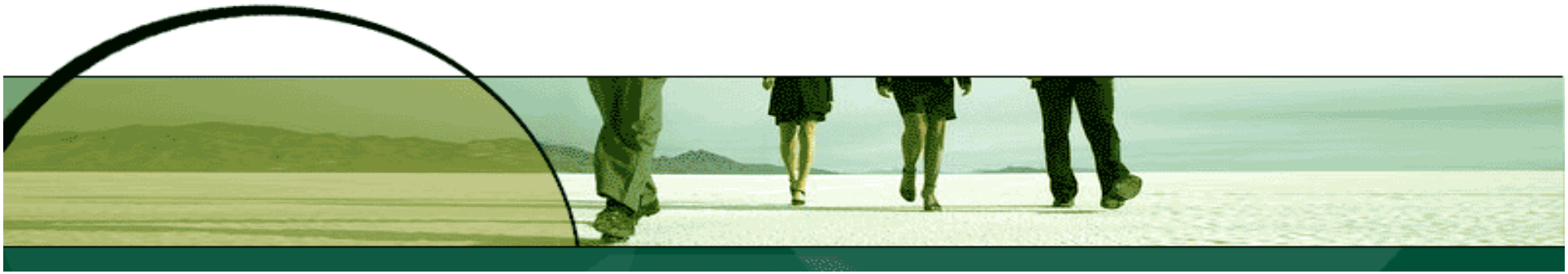
Email Marketing - CAN SPAM Act (con't)

Enforced primarily by FTC and state Attorneys General

- Also civil suits by ISPs and criminal provisions for falsification

Hefty Civil and Criminal Penalties:

- Imprisonment up to 5 years.
- Fines up to $3 million; fines may be higher if tied to actual damages incurred by recipients of fraudulent e-mail.
- Confiscation and forfeiture of any property (including computer hardware and software) used to commit crime, and any property traced to proceeds from crime.



CAN SPAM Act - Multiple Senders

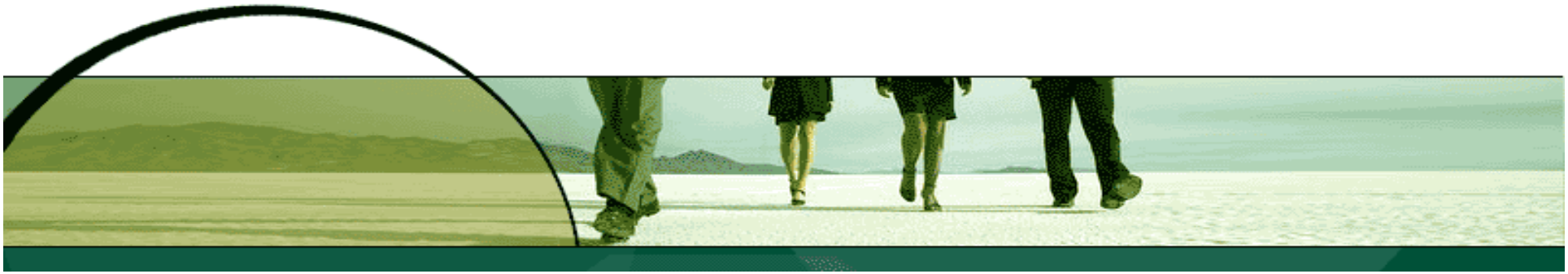
- Senders must honor opt-outs
- "Sender" is person who "initiates" a commercial e-mail message or procures the origination or transmission of the message and whose product, service, or Internet Web site is advertised or promoted by the message
- When more than one advertiser, all are deemed to be "sender" unless one party who meets definition also satisfies one or more of the following criteria:
  - controls message content;
  - determines email addresses to which message is sent; and/or
  - is identified as the sender in the "from" line.
- Addressed in FTC NPRM (2005)

FTC "Discretionary" CAN SPAM Rulemaking

- Rule for determining who is the "sender" in joint-marketing, advertiser, and other multiple sender contexts
- Rule for "Tell-a-Friend" messages
- Length of time that opt-out requests must be honored
  - from 10 business days to 3 business days?
- Still no final rule – waiting, waiting….

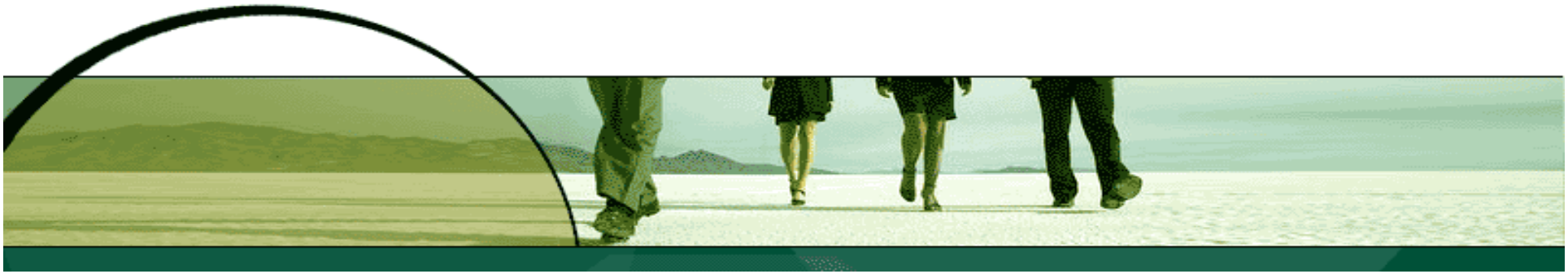
CAN SPAM – FTC Enforcement

- Recent increase in enforcement
- 2006 cases:
  - U.S. v. Jumpstart Technologies
  - FTC and California v. Optin Global
  - U.S. v. Kodak Imaging Network, Inc.
  - U.S. v. ICE.COM



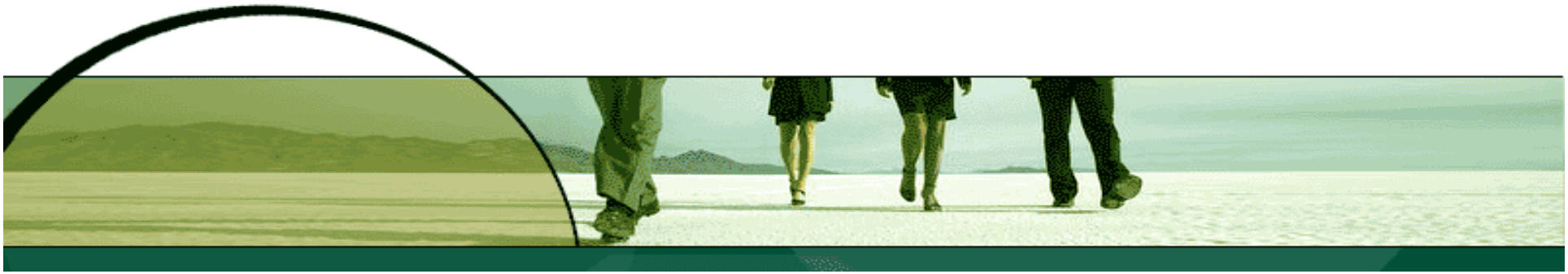
U.S. v. Jumpstart Technologies (2006)

- FTC charged Jumpstart with multiple violations of CAN SPAM:
  - To receive free prizes, individuals had to submit email address and 5 friends' email addresses
  - Jumpstart sent CEMs to individual's friends and masked them to look like they were sent by individual
  - Emails included note from individual as if he/she personally invited "friend" to participate
  - Small opt-out language at bottom
  - Didn't honor opt-outs
  - Forced to pay ***$900,000***



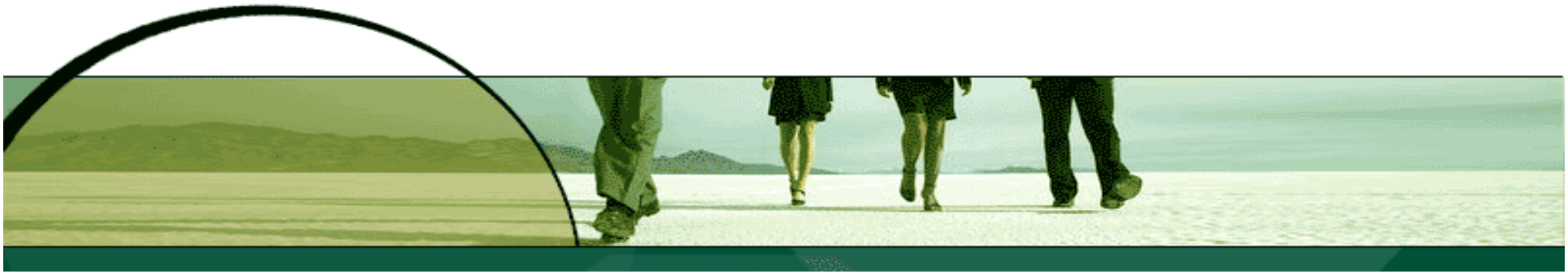
FTC and California v. Optin Global (2006)

- Optin Global transmitted hundreds of thousands of CEMs advertising many products and services
- Charged with numerous violations of CAN SPAM and CA deceptive trade practices law:
  - CEMs contained false header information
  - failed to notify recipients of their opt-out rights
  - contained deceptive subject headings
  - not identified as advertisements
  - failed to include sender's valid postal address
  - failed to honor opt-outs
- Optin had to pay ***$475,000 plus agree to review all future affiliate, partner and vendor email campaigns***



Be Careful when Dealing with Email List Brokers

- Recent state AG and federal enforcement actions illustrate obligation to ensure that email addresses purchased or rented from third parties were collected with proper notice
  - Email addressees must first be notified that unsolicited commercial emails may be sent to them
- Example: email marketer (Daltran Media) forced to pay $1.1 mi. to NY AG for buying “tainted” email addresses
- Email addresses cannot be “flipped” like commodities



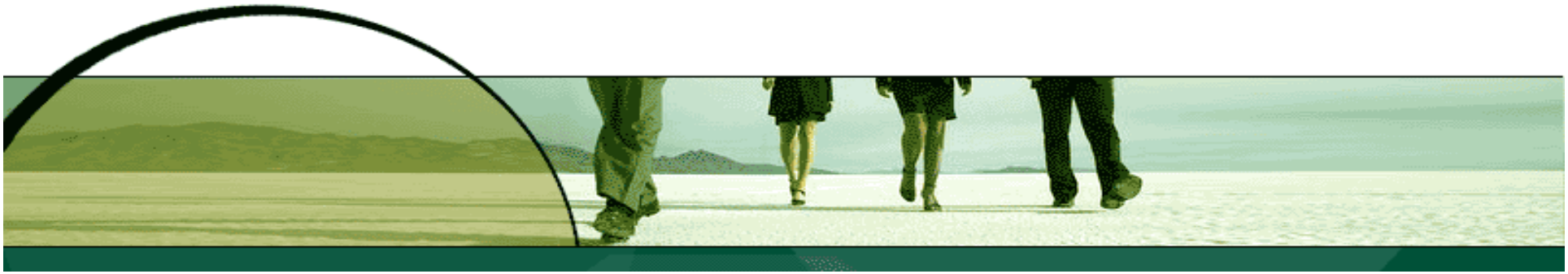
Mobile Marketing

Sending Marketing Messages to Wireless Devices

- E-mail ("Mobile Service Commercial Message") → CAN-SPAM
- Voice-Based Telemarketing →TCPA, TCFAPA, State Law
- Text Messaging (SMS) → TCPA, TCFAPA, State Law
- Short Code → Legal Framework Unclear

Mobile Marketing (con't)

- Mobile service commercial messages ("MSCMs")
  - Definition = e-mail sent to a wireless Internet domain name, where the primary purpose of the e-mail is commercial in nature
    - "wireless Internet domain name" = "7035551212@verizonwireless.net"
    - "Primary purpose" = depends on the content of the MSCM
    - "Transactional or relationship" MSCMs are excluded



Mobile Marketing (con't)

- MSCMs are prohibited absent "prior express authorization"
  - Can be oral, written or electronic (burden on sender)
  - Not transferable between affiliates
  - MSCM must be linked to specific purpose provided in notice
  - Other requirements (*e.g.*, cost free opt-out mechanism) apply
- Disclosures required for "prior express authorization"
  - Subscriber agrees; acknowledges potential wireless provider charges; can revoke at any time
  - Clearly disclose name of sender and entity whose product or service is being promoted
- These rules have minimized the use of MSCMs for purely promotional purposes

Mobile Marketing (con't)

- **Phone-to-Phone Text Messaging (SMS)**
  - Relies on subscriber's mobile phone number, not e-mail address, to transmit the message; thus,
    - SMS ≠ MCSM (so CAN-SPAM does not apply)
    - Federal and state voice-based telemarketing laws and regulations apply
      - Which ones?
      - Those governing autodialed and/or prerecorded calls

Mobile Marketing (con't)

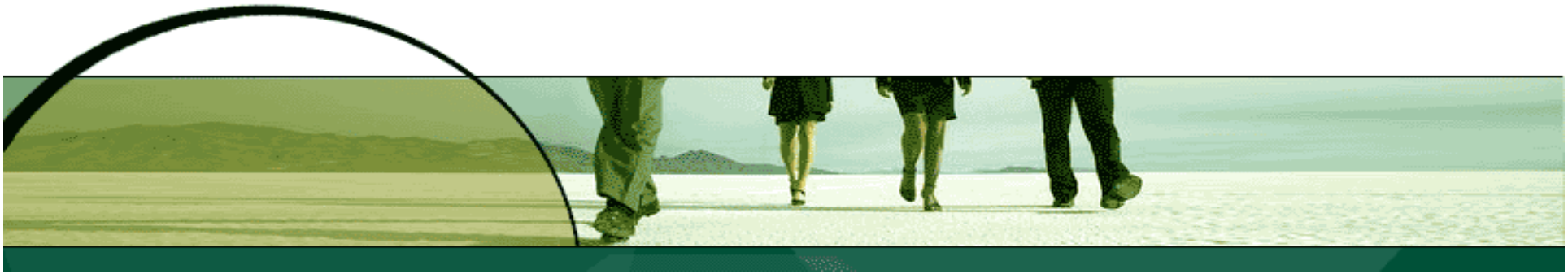
- **Phone-to-Phone Text Messaging (SMS)**
  - Autodialed/Prerecorded Call Regulations under TCPA:
    - Prohibited to mobile phones or any number for which the called party is charged absent "prior express consent"
    - "Prior express consent" = oral, written or electronic
    - Exception – wireless providers can send messages at no charge
  - All "telephone solicitations" to wireless devices must first be scrubbed against National Do Not Call list
    - Includes SMS text messages for purpose of encouraging purchase or rental of, or investment in, property, goods or services"
    - EBR exception
  - If a wireless number is on a company-specific Do-Not-Call list, don't call or send text message
    - No exceptions

Mobile Marketing (cont'd)

- **Phone-to-Phone Text Messaging (SMS)**
  - Numerous states have enacted disparate telemarketing regulations
  - Applicability to SMS can be unclear
    - *But see Joffe v. Acacia Mortgage Corp.*
  - Preemption issues are not fully resolved
    - Key provision = 47 U.S.C. § 227(e) (authorizes states to enact for restrictive *intrastate* regulations)
    - Case law is sparse and in conflict

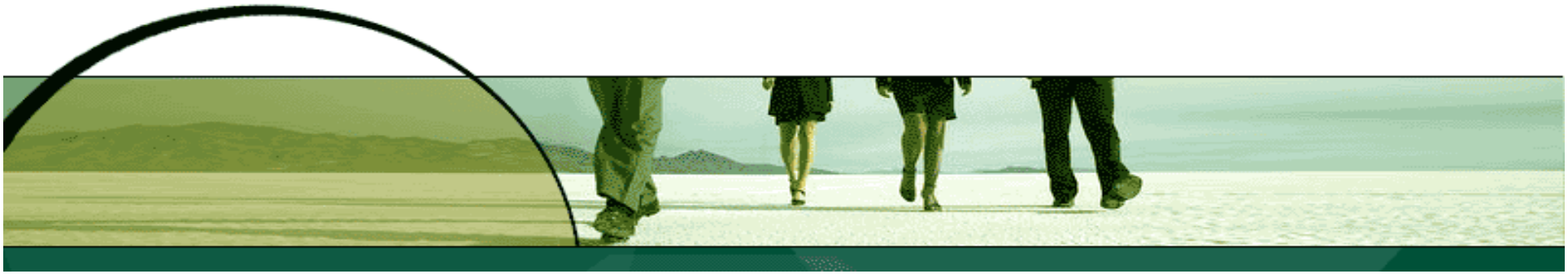
COPPA

- Children's Online Privacy Protection Act (COPPA) applies:
  - To commercial web sites that are **directed to children** under 13 and collect personal information from children or
  - A general audience web site that has **actual knowledge** that it is collecting personal information from children under 13



COPPA

- If applicable, COPPA requires:
  - A web site **privacy notice**
  - **Limited** collection of information
  - **Parental notification**, and in most cases, prior parental consent to collection/use/disclosure
  - **Parental Access**
  - **Security**

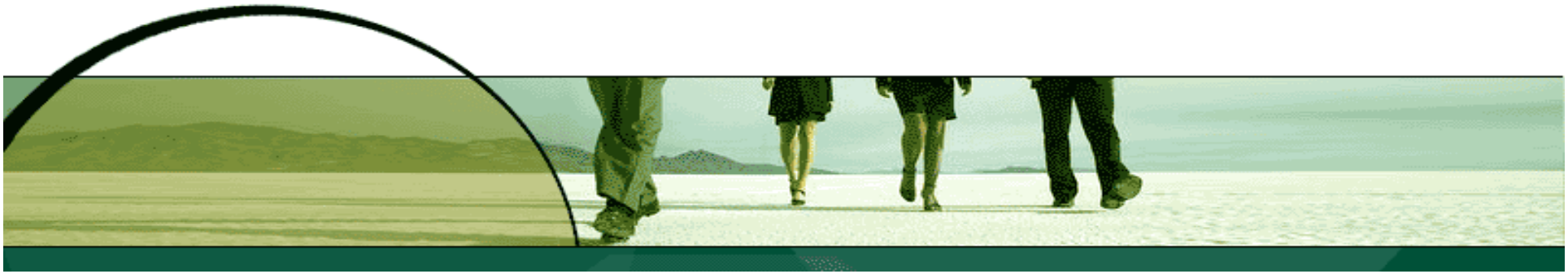


COPPA

- **Most Relevant Exceptions:**
  - If a site collects **only an email address** and the email address is used solely in connection with responding to a **one time request** of a child and the email address is then deleted
  - If a site collects only an email address and the email address is used solely in connection with responding to a **specific request from a child**, the site need only (prior to contacting the child more than once) provide parental notice and the **opportunity to object**

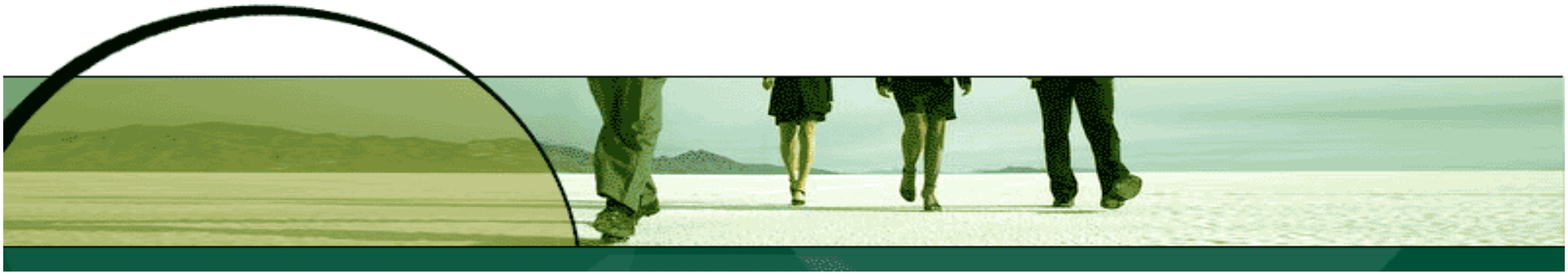
COPPA - FTC Enforcement

- Penalties are increasing - recent cases include settlements with:
  - Xanga for $1 mi. (2006)
  - UMG Recordings/Bonzi for $400K (2004)
  - Mrs. Fields for $100K (2003)
  - Hershey Foods for $85K (2003)
- Social networking sites should avoid collecting PII unless COPPA-compliant

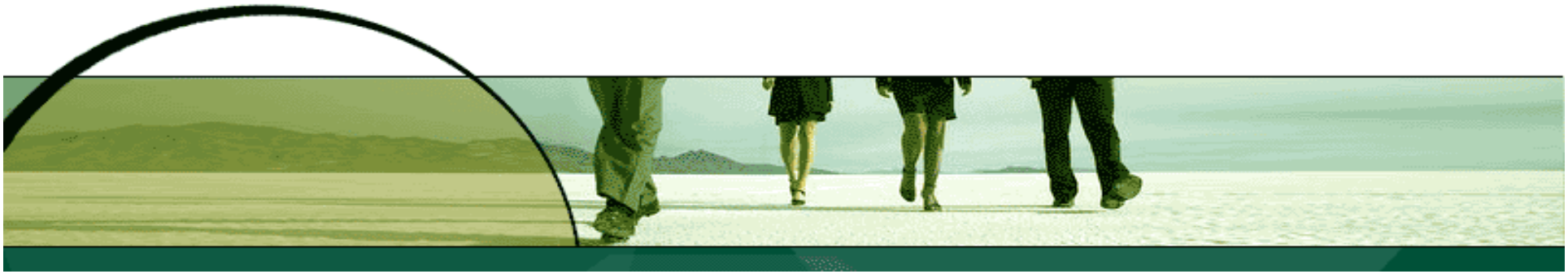


Part 4

A Look Ahead



- **A peer-to-peer network user whose Internet protocol address is visible to anyone using ordinary Internet software lacks a privacy interest in that address, even if the user has his or her file-sharing option switched off, the Minnesota Court of Appeals held April 17 in an unpublished decision.**
- **State of Minnesota v. Jacobs, 2007 ILRWeb (P&F) 1659 [Minn Ct App, 2007].**



Other Issues – Wireless Tracking

- Technology largely developed to comply with FCC regulations on wireless E911
- New and potential applications raise privacy concerns:
  - Location tracking as optional aspect of wireless service (e.g., for child/teen cell phones)
  - Location tracking as a requirement (e.g., for mountaineers)
  - Tracking of product usage (not just wireless communications devices but cars and other products)