

# **Current Trends in Coverage for Cyber Liability Risks**

**Tarron L. Gartner  
Cooper & Scully, P.C.  
900 Jackson Street  
Suite 100  
Dallas, Texas 75202  
(214) 712-9570 (direct)  
[tarron.gartner@cooperscully.com](mailto:tarron.gartner@cooperscully.com)**

© 2014 This paper and/or presentation provides information on general legal issues. It is not intended to provide advice on any specific legal matter or factual situation, and should not be construed as defining Cooper and Scully, P.C.'s position in a particular situation. Each case must be evaluated on its own facts. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act on this information without receiving professional legal counsel.

# Increased Use of Information Technology

- 65% of the global population are internet users;
- Global penetration of mobile/cellular subscriptions reached 97.5% in 2014;
- E-Commerce on line sales in North America has increased 460% since 2000; reaching \$212B in 2013;
- By the end of 2013, 80% of North American online sellers will expand into Brazil, Russia, India, Africa, Japan or China;
- By 2015, direct sales companies will generate 50% of sales through inbound marketing leads;
- Most internet retail and service providers use GPS location services enabled by phones to push personalized, location-based content to mobile devices for users who have subscribed to these services

# Knowledge is Power

- Information is a “commodity.” A commodity is “an article or raw material that can be bought or sold, especially a product as opposed to a service.
- If it can be bought, sold or traded, it can be accessed, stolen and used.
- The market for personal information is the fastest growing industry in the world, outpacing technology itself.
  - Legitimate use;
  - Black market.

# Cyber-Crimes on the Rise

- 2013\*
  - Successful cyber attacks per company per week: 122;
  - Average time to resolve cyber attacks: 32 days;
    - 130% increase from 2010.
  - Average cost to resolve a single attack: \$1M;
  - Average cost per day to resolve a cyber attack: \$32,469;
    - 55% increase from 2012 cost per day;
  - Annual average cost of cyber crime per company: \$11.6M.
    - Up from 6.5M in 2010.

\*Benchmark Samples of US Companies

Cited in presentation by Ernest Martin, Haynes & Boone, *Top Trends in Insurance Law*

The University of Texas School of Law, 18<sup>th</sup> Annual Insurance Law Institute, November 8, 2013

# Internet Law

- Concerns internet access and usage, privacy, freedom of expression and jurisdiction/sovereignty;
- Jurisdictional issues (think "Coverage Territory") involve:
  - the laws of the state/nation in which the user resides,
  - the laws of the state/nation that apply where the server hosting the transaction is located, and
  - the laws of the state/nation which apply to the person or business with whom the transaction takes place.

# Coverage Territory

- ISO amendatory endorsement form CG 00 24 22 04 13, effective May 1, 2014:
  - Provides for defense obligation under Supplementary Payment if “Suit” is brought in “coverage territory”;
  - Provides payments to be made in US Currency at the prevailing exchange rate (might be a bargain);
  - Defines “coverage territory” to mean “anywhere in the world with the exception of any country or jurisdiction which is subject to trade or other economic sanction or embargo by the United States of America.”

# Regulation

- **Law:** Conventional legislation governing issues such as gambling, child pornography, fraud, criminal conduct, corporate governance – same online as offline, with additional jurisdictional concerns. There can be criminal or civil implications, or both.
  - Privacy Act of 1974;
  - Electronic Communication Privacy Act;
  - Gramm-Leach-Bliley Act (allows financial institutions broad powers to share information with affiliates);
  - Homeland Security Act;
  - Digital Millennium Copyright Act\*;
  - Online Copyright Infringement Liability Limitation Act\*.

\*Criminal conduct enforced by CCIPS – Department of Justice

# Self-Regulation

- **Private internet-architectural products: and services:** Mechanisms to control the transmission of information , including internet filtering software, encryption programs, spam filters, server hosts, site sponsors, etc.;
- **Markets:** Economic and political markets who may use the information and who may ultimately control the information;
- **Net Neutrality:** Control of the transmission of data through routers and infrastructure owned by a collection of private and public entities, including telecommunications companies, universities, and governments, designed to allow equal access to information by internet users.

▪

# Net Neutrality

- State of the Net Conference – Governmental Caucus of Congressional members who met to discuss the Federal Government's Internet-related priorities. Agenda included:

- Status of proposed legislation by FCC for cyber-security, a rewrite of the 1996 Communications Act, reforming federal electronic-surveillance laws.
- Net Neutrality – *Verizon/MetroPCS v. FCC* (No. 11-1355 (D.C. Cir.) suit involving the legality of the FCC's "Open Internet" order, more commonly known as the Net Neutrality Rule, which prohibits ISPs from blocking lawful web content. (i.e. Rules prevent provider from blocking *lawful* web content that competes with the provider's own services).

# Net Neutrality

- District Court's ruling: The FCC does not have the authority to enforce the rules on Internet service providers because it did not classify broadband Internet service as a telecommunications service.
  - Could be resolved by classifying broadband service into the same category as more highly regulated phone service.
- FCC is to propose new rules in late spring or early summer that will:
  - Fulfill key components of net neutrality without reclassifying broadband service.
  - Ensure that Internet service providers don't discriminate against different types of content, particularly by favoring their own services, such as movie streaming, over those of competitors.
  - Try to guarantee an open Internet by enhancing and enforcing its rules requiring network operators to disclose how they manage Internet traffic.

# Right of Privacy

- Reasonable expectation of privacy - *Katz v United States*, 389 U.S. 347 (1967).
  - A person must exhibit an "actual (subjective) expectation of privacy";
  - "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"
- Privacy Act of 1974;
- Foreign Service Intelligence Act;
- Electronic Communication Privacy Act;
- Gramm-Leach-Bliley Act (allows financial institutions broad powers to share information with affiliates);
- Homeland Security Act (enforces Privacy Act).

# ICANN and ITU

- Internet Corporation for Assigned Names and Numbers: U.S. – based non-profit organization responsible for the coordination of the global Internet's systems of unique identifiers, including coordination of the internet protocol and address spaces, for the management of the top-level domain name space, and the development and maintenance of the DNS (domain name system) for (domestic and international) generic top-level domains.
- International Telecommunications Union: UN agency responsible for issues that concern information and communication technologies, including radio spectrum and satellite orbits, the development and standardization of international networks and technologies to improve communication access to underserved countries.
- Two weeks ago the Department of Commerce would be VOLUNTARILY relinquishing control of ICANN: “Convening stakeholders across the global Internet community,” with ICANN participating to “craft an appropriate transition plan.” Los Angeles Times, March 26, 2014.  
–WHO?

# Risks

## ■ Commercial Risks

- Viruses that infiltrate the user's computer to target site specific (financial) locations in order to access login information (through tracking login keystrokes) in order to perpetrate direct theft, identify theft and the purchase of goods with the user's personal information;
- Viruses that overwhelm the server's system, during which data stored on the server's host site is stolen;
- Piracy (theft of intellectual property, illegal music and video downloads);
- "Reverse engineering" of manufactured products using product data stored in usable and unusable form;
- Interception of funds transferred funds;
  - Bank of America – no transfer of funds over seas w/o special account.
- Hacking of personal information to sell to people who will use it for anything from targeted advertising to theft.

## ■ Personal Risks

- Cyber-Stalking;
- Cyber-Bullying;
- Defamation;
- Identity Theft
- Illegal use of intellectual property

# TRADITIONAL POLICIES

- Commercial Package Policies, including employee theft, employee dishonesty; property;
- Commercial General Liability Policies;
  - Coverage A – Bodily Injury and Property Damage Liability;
  - Coverage B – Personal and Advertising Injury Liability;
- D&O and E&O Policies;
- Fidelity Policies;
- Homeowner's Policies, including property and liability coverage.

# Traditional Policies Address Traditional Risks

- CGL (Coverage A) and Homeowner's Liability Policies insure against liability for "bodily injury" and "property damage" caused by an "occurrence" or an accident;
  - Cyber-torts are not typically "accidental";
  - Mental anguish is not typically "bodily injury";
  - Information is not typically "tangible property";
  - Exclusions for liability arising out of loss of electronic data;
- Property Policies typically provide coverage for "property damage";
  - Loss of electronic data is not "property damage";
  - Low sub-limits of liability;
  - Often endorsed to exclude loss of electronic data;
  - Coverage is typically limited (higher sublimit) for employee theft and dishonesty.

## Current Loss of Information is Not “Property Damage”

Tangible property” is property that is capable of being handled, held or touched. *See State Auto Property and Cas. Ins. Co. v. Midwest Computers & More*, 147 F.Supp.2d 1113 (W.D. Ok. 2001); *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4<sup>th</sup> Cir. 2003); *Recall Total Information Management*, 2012 WL 46988 (Ct. Super, January 17, 2012).

# Traditional Policies Address Traditional Risks

- CGL (Coverage B) Policies insure against liability for “personal and advertising injury”;
  - “personal injury” liability includes defamation;
  - “Advertising injury” must arise out of insured’s advertisement;
  - Broad exclusions for intellectual property torts;
- Many Homeowner’s Policies exclude coverage for “personal injury” claims;
- D&O and E&O Policies insure against “wrongful acts”
  - Usually “claims-made and reported” forms;
  - Eroding limits (accelerated erosion of limits in defense costs);
  - Exclusions for loss of electronic data;
  - Exclusions for fraudulent, malicious, criminal, dishonest conduct by “any” insured.”

# Conflation of Terms "Personal and Advertising Injury"

- False, arrest, detention or imprisonment;
- Malicious prosecution;
- The wrongful eviction from, wrongful entry into, or invasion of the right of private occupancy of a room, dwelling or premises that a person occupies, committed by or on behalf of its owner, landlord, or lessor;
- Oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services'
- Oral or written publication of material that violates a person's right of privacy;
- Copying, in your "advertisement", a person's or organization's "advertising idea" or style of "advertisement";
- Infringement of copyright, slogan or title of any literary or artistic work, in your "advertisement".

## What Type of "Personal and Advertising Injury" Claims Might Be Covered?

- Vicarious liability for employee who illegally downloads music (if within scope of employment);
- Vicarious liability for employee who illegally downloads music (if within scope of employment);
- Blogging by employees (defaming competitor products, or use of company email or blogging as a personal diary);
- Data breach, if it results in theft of intellectual property and later used in insured's "advertising activities";
- Theft of customer data may be a "publication of material that violates a person's right of privacy." See *Norfolk & Dedham Mut. Fire Ins. Co. v. Clearly Consultants, Inc.*, 81 Mass.App.Ct. 40 (Dec. 16, 2011). But See *Creative Host. Ventures, Inc. v. E.T. Ltd., Inc.*, 2011 U.S. App. 19990 (Sept. 30, 2011).

# *Zurich v. Sony*

- Claim involved Sony's liability for theft (by hacking) of personal information of X-Box users;
- Court ruled from bench that claims were not "publication of material that violates a person's right of privacy" because Sony didn't "publish";
- Sony's policy defined personal injury publication of material that "in any manner" violated a person's right of privacy.

# Current Exclusions

- Exclusion p – Electronic Data – Modified in 2013 Form
- Recording and Distribution of Material or Information in Violation of Law:
  - Applies to “personal and advertising injury that violates:
    - TCPA (fax blasts);
    - CAN-SPAM Act of 2003;
    - Fair Credit Reporting Act;
    - Any federal, state or local statute ordinance, law or regulation...that prohibits or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information.

# New ISO Endorsements Effective May 1, 2014

- CG 00 01 04 13 – Electronic Data Exclusion:
  - p. Electronic data

Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access or inability to manipulate electronic data.

However, this exclusion does not apply to liability for damages because of "bodily injury."

As used in this exclusion, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

# NEW ISO FORMS

- Access or Disclosure Of Confidential Or Personal Information  
Damages arising out of:

Any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit care information, health information or any other type of nonpublic information; or

The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

This exclusion applies even if damages are claims for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of that which is described in Paragraph (1) or (2) above.

- Same wording for "personal and advertising injury" claims.

# Coup D'état

- CG 24 13 04 13 – Amendment of Personal and Advertising Injury Liability

“With respect to Coverage B Personal and Advertising Injury Liability, Paragraph 14.e of the Definitions Section does not apply.”

# New Products –ISO FORMS

- **Website publishing liability provides coverage against Internet-related publishing perils, including libel against a person or organization, and copyright, trademark, and service mark infringement allegations arising out of content published by the policyholder on its website.**
- **Network security liability covers the policyholder against claims for failing to maintain the security of a computer system resulting in unauthorized access and publication of personal information, such as credit card numbers or personal medical information.**
- **Replacement or restoration of electronic data provides coverage for the cost of replacing or restoring electronic data lost or rendered inaccessible because of an e-commerce incident, such as a virus, malicious instruction or denial-of-service attack.**
- **Cyber extortion provides coverage for extortion expenses incurred and ransom payments made because of an extortion threat. Extortion is defined as a threat to commit an e-commerce incident, disseminate the policyholder's proprietary information, reveal a weakness in its source code or publish personal information belonging to policyholders' clients.**
- **Business income and extra expense provides coverage for loss of business income or extra expenses incurred as a result of an extortion threat or e-commerce incident.**