Courageous Counsel Leadership Institute

Navigating Business in a Global Economy

November 29, 2016
St. Regis Hotel
New York, NY

大成 DENTONS

Internet login Information

Username: StRegisMeetingRooms

Password: Dentons2016

1. Log onto The St. Regis network

2. Open web browser and go to a www.website
   i.e. www.google.com

3. You will get directed to The St. Regis splash page to enter access code

Special thank you to the Courageous Counsel Leadership Institute Advisory Board for their dedication and commitment.

Janice Block, Executive Vice President and Chief Legal and Administrative Officer, Kaplan Inc.
Michele Coleman Mayes, Vice President, General Counsel and Secretary, New York Public Library
Lucy Fato, Managing Director, Head of the Americas and General Counsel of Nardello & Co.
Gloria Santona, Executive Vice President, General Counsel and Secretary, McDonald's Corporation
Heidi M. Wilson, Senior Vice President, General Counsel and Corporate Secretary, Tennant Company

Navigating Business in a Global Economy

大成 DENTONS

COURAGEOUS COUNSEL

Navigating Business in a Global Economy
November 29, 2016
St. Regis Hotel
New York, NY

Table of Contents

Tab 1

大成 DENTONS

COURAGEOUS COUNSEL

Navigating Business in a Global Economy
November 29, 2016
St. Regis Hotel
New York, NY

Agenda

7:45–9 a.m.	**Registration and networking breakfast**
9–9:20 a.m.	**Welcome** Kara Baysinger, Partner, Dentons; co-author of *Courageous Counsel: Conversations with Women General Counsel in the Fortune 500* **Opening remarks:** The Clash Between Globalization and Cultural Identity Elliott Portnoy, Global Chief Executive Officer, Dentons Joe Andrew, Global Chairman, Dentons
9:25–9:55 a.m.	**Introductory keynote** Introduction: Mary Ann Hynes, Senior Counsel, Dentons Keynote: Gloria Santona, Executive Vice President, General Counsel and Secretary, McDonald's Corporation

10–11 a.m.	**General session** Navigating Cybersecurity in a Global Economy: From Prevention to Breach Response Moderator: Chantal Bernier, Counsel, Dentons Panelists: Dennis Garcia, Assistant General Counsel, Microsoft Aparna Williams, Director of Global Selling Programs and Channels, Legal and Public Affairs, Symantec Corporation.
11–11:15 a.m.	**Networking break**
11:15 a.m.–12:15 p.m.	**General session** Globalization: Operating Your Business on the Global Stage Moderator: Jana Cohen Barbe, Global Vice Chair, Dentons Panelists: Wendi Glassman, Vice Chairman of Legal Affairs and Corporate Secretary, Bank Leumi USA Lucy Fato, Managing Director, Head of the Americas and General Counsel, Nardello & Co. Kim Yapchai, Chief Compliance Officer, Whirlpool Corporation
12:30–2 p.m.	**Lunch and keynote** Introduction: Natalie Spears, Partner, Dentons Keynote: Leigh Weinraub, Mind in Motion
2:05–3:05 p.m.	**Track 1** **Endgame: Limitation of Liabilities** A contract's limitation of liabilities clause is the endgame of every negotiation. This session will take a comprehensive, tactical approach to limiting liabilities, including key challenges and common missteps and misconceptions. Panelists: Stafford Matthews, Partner, Dentons Susan Greenspon, Partner, Dentons **Track 2** **Negotiating Successful Outcomes: How to Influence and Impact Big-Ticket Mediations and Settlements in the US and Abroad** Key tips for negotiations, the role of the GC in mediations and meetings with regulators, different angles of preparation with key stakeholders in your company, cultural factors in global dispute resolutions, and properly valuing your case. Moderator: Natalie Spears, Partner, Dentons Panelists: Janice Block, Executive Vice President and Chief Legal and Administrative Officer, Kaplan Inc. Hon. Shira Scheindlin (Ret.), JAMS; former United States District Court Judge for the Southern District of New York Megan Belcher, former Vice President and Chief Counsel for Employment Law and Compliance, ConAgra Foods

	Track 3 **Protecting Your IP** Whether it be through trademarks, patents, trade secrets or other alternatives, it is critical to have a strategy in this era of data breaches, globalization, ease of movement of the workforce and ever-changing laws. Moderator: Ira Kotel, Partner, Dentons Panelists: Deidra Gold, Executive Vice President and General Counsel, Wolters Kluwer United States Inc. Heather Khassian, Counsel, Dentons Annemarie Brennan, Vice President and Associate General Counsel, NAM, Sivantos Group
3:10–4:10 p.m.	**General session** Post-Election Panel Moderator: Kara Baysinger, Partner, Dentons, and co-author of *Courageous Counsel: Conversations with Women General Counsel in the Fortune 500* Panelists: Kathleen O'Connor, Counsel, Dentons Governor Howard Dean, Senior Advisor, Dentons
4:10–4:25 p.m.	**Networking break**
4:25–5:25 p.m.	**General session** Designing Your Role: Creating the Role You Want by Building Your Team and Negotiating Your Title and Pay Moderator: Michele Coleman Mayes, Vice President, General Counsel and Secretary, New York Public Library; co-author of *Courageous Counsel: Conversations with Women General Counsel in the Fortune 500* Panelists: Mary Ann Hynes, Senior Counsel, Dentons Catherine Nathan, Partner and former Co-Head of Legal, Compliance and Regulatory Practice, Spencer Stuart Cheryl Beebe, former Executive Vice President and Chief Financial Officer of Ingredion Incorporated; board of directors, various corporations
5:25 p.m.	**Wrap-up**

Tab 2

大成 DENTONS

COURAGEOUS COUNSEL

Introductory Keynote Speaker

Gloria Santona is the Executive Vice President, General Counsel and Secretary of McDonald's Corporation. Tasked with anticipating conflicts and protecting the McDonald's brand across the globe, she oversees the company's global legal, compliance and regulatory teams. She also works closely with McDonald's independent Board of Directors as their liaison to senior management.

Well-versed in the challenges facing the brand after three decades with McDonald's, Santona held several leadership positions, including Corporate Secretary and U.S. General Counsel, before becoming Corporate General Counsel in 2001. To drive McDonald's evolving business priorities, Santona challenges her teams to balance their legal expertise with business acumen.

Widely respected in the legal profession, Santona was named an Outstanding General Counsel by the National Law Journal in 2016. Among other awards, she has been recognized as one of America's Top General Counsels by Corporate Board Member magazine. Under Santona's leadership, McDonald's legal department has been recognized for its commitments to women and diversity.

Santona provides thoughtful insight into corporate governance, which comes, in part, from her roles on the Boards of Directors for other businesses and organizations. She is a member of the Board of Directors of Aon PLC, the Greater Chicago Food Depository and a trustee of Rush University Medical Center.

Santona earned a Bachelor of Science degree from Michigan State University and a Juris Doctor from the University of Michigan Law School, graduating cum laude.

大成 DENTONS

COURAGEOUS COUNSEL

Luncheon Keynote Speaker

Leigh Weinraub is an innovative pioneer in the world of personal transformation. As an internationally acclaimed speaker, entrepreneur, author and competitive athlete Leigh helps people unlock their inner-strength to become their own greatest champion.

Leigh rose from one of America's top junior tennis players, to scholarship athlete to coaching of Dartmouth and Northwestern University. After earning her Masters in counseling psychology from Northwestern, Leigh built a thriving private practice using her innovative WALK AND TALK THERAPY.

Springing from a passion for helping others create a destiny of their own choosing, today Leigh is the founder of Mind in Motion, a universal movement and lifestyle brand. In addition to speaking, she has created an innovative apparel line that motivates and inspires people to get off the couch and move their mind and body.

"Our bodies instinctively know how to self heal and if we give them half a chance they can heal our minds as well," Leigh promises. "So lace up your shoes, kick the therapy couch to the curb and let the momentum of a walk carry you forward into the change you crave."

大成 DENTONS

COURAGEOUS COUNSEL

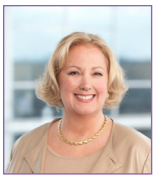
Speakers

Kara Baysinger is a San Francisco-based partner at Dentons, where she heads the Firm's global Insurance practice and Insurance Regulatory practice. She also serves as a key member of the Firm's leadership team. Kara is sought after to help insurers solve their most complex, mission critical and/or sensitive business and regulatory issues, based on her strong and successful career in private practice and her years spent in-house at insurance companies. On top of a demanding practice, Kara is actively involved in the Firm's women's initiative, Dentons' Women LEAD. She has always viewed workplace diversity and women's advancement as a calling. In 2011, Kara co-authored Courageous Counsel: Conversations with Women General Counsel in the Fortune 500, a volume tracing the career arc of 42 women general counsel at some of America's largest corporations.

Jana Barbe serves as Global Vice Chair of Dentons, the largest law firm in the world. Since the inception of Dentons, Jana has been integrally involved in the development and implementation of a strategic vision that created this top tier global legal business. Jana is also widely acknowledged as one of the most influential and highly regarded practitioners in real estate law and represents many of worlds the largest financial institutions and insurance companies on their social and community investing programs.

Chantal Bernier joined the Privacy and Cybersecurity practice of Dentons Canada LLP in 2014 after nearly 6 years leading the Office of the Privacy Commissioner of Canada (OPC) as Interim Privacy Commissioner and as Assistant Commissioner

Prior to this, Chantal worked as Assistant Deputy Minister for Socio-Economic Development at Aboriginal and Northern Affairs Canada, Assistant Deputy Minister for Community Safety and Partnerships at Public Safety Canada, and Director of Operations for the Machinery of Government Secretariat of the Privy Council Office.



Cheryl Beebe was responsible for all aspects of Ingredion's financial operations, including financial planning, treasury, tax, accounting, risk management, investor relations, insurance, corporate communication and internal audit. She is a 30+ year veteran of the company and has served in a number of positions including senior advisor to the CEO, chief financial officer, vice president finance, and corporate treasurer since the inception of Corn Products International in 1998. Cheryl joined the company when it was part of CPC International in 1980 and served in various positions in CPC's U.S. consumer food business, North American audit group and worldwide corporate treasury group.

Megan Belcher was most recently Vice President & Chief Counsel – Employment Law and Compliance for ConAgra Brands, a Fortune 250 consumer foods company. In her position, she led the team of attorneys and professionals who handled the labor, employment, and benefits legal work for the company, which included managing all employment litigation nationally and internationally. In addition, she created and led the company's enterprise-wide compliance initiative. Prior to joining ConAgra Foods in 2007, Megan was a litigator with an Am Law 200 law firm.

Janice Block is an executive vice president and the Chief Legal and Administrative Officer, at Kaplan Inc., a global education company owned by The Graham Holdings Company. As Kaplan Inc.'s Chief Legal and Administrative Officer, Janice leads a worldwide team of legal, regulatory, compliance, government relations, human resources and talent development professionals, supporting all facets of Kaplan's business. She also serves on the board of directors and as an officer of numerous Kaplan entities in the U.S. and overseas.

Annemarie Brennan is Sivantos, Inc.'s Associate General Counsel for North America. Sivantos was formerly the global audiology division of Siemens, AG. The division was divested by Siemens in January 2015 to the private equity firm EQT and re-named Sivantos. Before joining Sivantos in 2012, Annemarie was an Assistant General Counsel with C.R. Bard, Inc. and an Associate General Counsel with Matheson Tri-Gas, Inc. Prior to moving in-house Annemarie spent ten years in private practice in Washington, DC.

Governor Howard Dean is a Senior Advisor in the Public Policy and Regulation practice at Dentons. He focuses on health care and energy issues, as well as providing expertise derived from his extensive experience in public office.

Governor Dean comes to Dentons after serving as Chairman of the Democratic National Committee, where he created and implemented the "50 State Strategy", encouraging the cultivation of candidates in every state at every level, rather than solely the traditionally democratic-leaning states.

Dennis Garcia is an Assistant General Counsel for Microsoft based in Chicago. He leads the legal support function to Microsoft's U.S. Central Region Enterprise & Partner Group team. Prior to joining Microsoft, Dennis worked as an in-house counsel for Accenture and IBM. Dennis received his B.A. in Political Science from Binghamton University and his J.D. from Columbia Law School. He is admitted to practice in New York, Connecticut and Illinois (House Counsel).

Wendi G. Glassman is the Vice Chairman--Legal Affairs and Corporate Secretary of Bank Leumi USA, the largest subsidiary of the Leumi Group, one of the largest banking groups in Israel. She has served as counsel to Bank Leumi for 33 years. She joined as the senior counsel for Leumi's Regional Management in the Western Hemisphere. In 1993, she also joined Bank Leumi USA as its Corporate Secretary. Since 1998 she served as Bank Leumi USA's General Counsel and Corporate Secretary, responsible for all legal matters for the bank and the board of directors.

Deidra Gold is the Executive Vice President and General Counsel of Wolters Kluwer United States Inc. and various affiliated Wolters Kluwer companies. In that role, she serves as the chief legal officer for the Company's operations throughout the Americas. She also oversees legal work on various multi-national projects for Wolters Kluwer N.V. and is a member of its Senior Management Council. Before joining Wolters Kluwer in late 2005, Deidra served as an executive officer of a number of public companies (including Ameritech, Essendant and Premier Farnell) and as a partner in two law firms. Deidra has a J.D. from Columbia University School of Law, and an M.B.A. from the J.L. Kellogg Graduate School of Management at Northwestern University.

Susan Greenspon focuses her practice on financings, mergers and acquisitions, corporate governance matters and general corporate counseling in the United States and worldwide. Susan's experience on working with international companies and US-based companies with foreign operations has enabled her to assist her clients in structuring their corporate entities and restructuring them when needed. Her clients span a wide range of industry sectors, including several of the largest global pharmaceutical companies, software developers; Internet and technology companies, including green technology companies; skin care, hair care, salons spas and cosmetic entities, commercial and resort real estate developers and brokerage firms; manufacturers; private boarding schools; publishers and distributors; and retailers of home decorating products and commercial and electronic components.

Mary Ann Hynes is a Senior Counsel at Dentons. She is an innovator and trailblazer for the advancement of women in high ranking corporate legal positions and has served as General Counsel or Chief Legal Officer for Sundstrand Corporation, CCH, Ingredion (formerly known as Corn Products International), IMC Global and WoltersKluwer. She has experience in the areas of governance, compliance, and mergers and acquisitions, with a special focus on international growth, innovation, strategy and risk management. Mary Ann was also a Non-Executive Director of GHD Group Pty Ltd. She has been a board member of several corporations and nonprofit organizations, such as the Dr. Scholl Foundation and the John Marshall Law School, a frequent industry speaker, and an advocate of opportunities for women in law and championing the cause of diversity in the legal profession.

Heather Khassian is a member of Dentons' Intellectual Property and Technology group in Houston, Texas. Heather's practice involves managing IP portfolios consisting mostly of patents, trade secrets, and trademarks for clients in multiple technology sectors, doing deals involving IP for companies of all sizes, and litigating patent and trade secret cases in Federal Court. Heather is passionate about legal ethics and regularly speaks on ethics issues and serves on the firm's pro bono committee.

Ira Kotel is a NY-based partner in Dentons' Venture Technology and Emerging Growth Companies practices. His practice encompasses all major transactional areas, including M&A, securities, venture capital, strategic alliances and technology licensing. He regularly serves as outside general counsel to emerging growth and middle market companies. In addition to overseeing their day-to-day corporate counseling needs, he also provides strategic and governance advice on a variety of major business transactions for clients both domestically and internationally.

Michele Coleman Mayes is Vice President, General Counsel and Secretary for the New York Public Library (NYPL). Ms. Mayes became Chair of the Commission on Women in the Profession of the American Bar Association in August 2014. Effective in 2015, she was appointed as an Advisor to the ABA Business Law Section, and in that same year, became a Fellow of the American College of Governance Counsel. In August 2016, she was elected to the Board of Directors of Gogo Inc.

Stafford Matthews is a technology transactions and intellectual property lawyer and the managing partner of the Silicon Valley office of Dentons. He is US Co-Chair of Dentons Global Technology Media and Telecommunications (TMT) Sector and has been recognized by the US Legal 500 in Venture Capital and Emerging Companies. Mr. Matthews is one of only 11 lawyers in the United States selected as a 2016 BTI Client Services All-Star in the field of Competition and Antitrust Law. He is dual qualified as an English solicitor and a US lawyer.

Catherine Nathan is a lawyer and a member of Spencer Stuart's Legal, Compliance & Regulatory and Education, Nonprofit & Government practices. Since entering search in 1988, Catherine has developed a successful retained legal search business, recruiting general counsel, senior in-house lawyers and partners for major corporations, nonprofit organizations and professional services firms. She also is the former leader of the firm's Legal, Compliance & Regulatory Practice in North America and co-leader of the practice globally.

Kathleen O'Connor is a member of the Public Policy and Regulation practice of Dentons in the firm's New York and Albany offices. With over 20 years of experience working in and around government, Ms. O'Connor has a unique understanding of the intersection of business and government. She assists clients in developing and implementing strategies to achieve their public policy objectives, including drafting and monitoring legislation, and regularly appears before executive and agency levels of government.

Hon. Shira A. Scheindlin (Ret.) joins JAMS after serving for 22 years as a United States District Judge for the Southern District of New York. Judge Scheindlin previously worked as a prosecutor (Assistan United States Attorney for the Eastern District of New York), commercial lawyer (General Counsel for the New York City Department of Investigation and partner at Herzfeld & Rubin), and Judge (Magistrate Judge in the Eastern District of New York 1982-1986 and Special Master in the Agent Orange mass tort litigation). Judge Scheindlin is known for her intellectual acumen, and expertise in mass torts, electronic discovery, civil rights, constitutional, and complex litigation.

Natalie Spears is a trial lawyer and represents clients in state and federal courts across the US in a wide range of matters, including consumer class actions, IP, media and advertising disputes, complex commercial and real estate litigation. As a member of Dentons' US Board and head of its global Technology, Media and Telecommunications sector, Natalie sets direction for the firm's commitment to exceptional client service. Her representative clients include major global media and entertainment, retail, real estate and consumer products and services companies.

Aparna Williams is currently a director in the Legal and Public Affairs department at Symantec Corporation. A graduate of the University of Maryland Baltimore County and the University of North Carolina Chapel Hill School of Law, she stumbled into in-house work almost immediately with software and related technology as the main focus, having been with Symantec in different legal roles since 2000. Aparna is a member of the Maryland, Virginia and District of Columbia bars. She is a proponent of providing agile and effective legal support in an ever-evolving global economy. Additionally, she serves on the board of the Pride Hockey Association, supporting young female ice hockey athletes in their pursuit of athletics and education.

Kim Yapchai, chief compliance officer of Whirlpool Corporation, helps maintain the company's reputation for high integrity which inspires stakeholder confidence and encourages speaking up. Her team focuses on building confident and educated business teams who understand risks and make smart, compliant decisions. Kim is known for her ability to work proactively with clients to find practical solutions. Before joining Whirlpool, Kim was assistant general counsel at Masco Corporation and began her career at Ford Motor Credit Company.

Tab 3

大成 DENTONS

Courageous Counsel Leadership Institute

COURAGEOUS COUNSEL

Navigating Business in a Global Economy
November 29, 2016
St. Regis Hotel
New York, NY

Attendee List

First Name	Last Name	Job Title	Company
Randi	Pollack	Vice President and Digital Media Counsel	A&E Television Networks LLC
Jill	Greenwald	Assistant Chief Counsel	ABC Television
Kelly	Galligan- DiCapua	Vice President and Associate General Counsel	AIG Global Real Estate
Kristen	Gudewicz-O'Neill	Associate General Counsel and Vice President	AIG Investments and Financial Services
Dana	Rosen	General Counsel	ALM Media Properties LLC
Gina	Okum	Chief IT Legal Officer & Associate General Counsel	American International Group, Inc. (AIG)
Cynthia	Patton	Vice President, Law, Global Commerical Operations	Amgen Inc
Linda	Rush	Privacy Officer and Associate General Counsel	Avis Budget Group Inc
Sapna	Maloor	Senior Director and Counsel	Axa Equitable Life Insurance Company
Jill	Rafaloff	Lead Director / Associate Gen Cnsl	Axa Equitable Life Insurance Company

First Name	Last Name	Job Title	Company
Mohana	Terry	Senior Director and Counsel	Axa Equitable Life Insurance Company
Allie	Lin	Senior Director & Counsel	AXA Insurance Company
Wendi	Glassman	General Counsel and Corporate Secretary	Bank Leumi USA
Helen	Walper	Head of Legal	Barclays Capital Inc
LaTanya	Langley	Vice President and General Counsel	BIC International Co.
Bindu	Cudjoe	Deputy General Counsel and Administrative Officer	BMO Financial Group
Efe	Ukala	Attorney	Borah, Goldstein, Altschuler, Nahins & Goidel, PC
Marcela	Kopelman	Corporate Counsel-BGS	Brink's U.S.
Tami	Stevenson	General Counsel	Broadspire Services Inc
Janet	Dhillon	Executive Vice President, General Counsel and Corporate Secretary	Burlington Coat Factory
Laura	Kilian	Assistant General Counsel	BuzzFeed Inc
Helene	Ashenberg	Partner	Capstone Partnership
Rebecca	Collins	Associate General Counsel, Corporate Affairs	Chubb
Sara	Garvey	Chubb Commercial Counsel	Chubb
Elizabeth	Aylett	Senior Counsel and Director	Cibc World Markets Corporation
Anamika	Samanta	Executive Director Counsel	Cibc World Markets Corporation
Rosa	Yun		Cibc World Markets Corporation
Amy	Lazzaro	Vice President of State Public Policy and Regulatory Affairs	Cigna
Kathleen M.	Cronin	Managing Director and General Counsel	CME Group Inc
Carrie	Di Santo	Managing Director and Global Chief Compliance Officer	CME Group Inc
Brigette	McLeod		Colgate-Palmolive Company
Kathleen	Fong	VP, CLO and Secretary	Conair Corporation
Julie	Gackenbach	Principal	Confrere Strategies LLC
Wendy	Weingart	Vice President, General Counsel and Human Resources	CORE Services Group Inc
Anne	Shean	Managing Director of Credit Loan Risk Review	Crédit Agricole Corporate and Investment Bank
Sarah	Nelson	Vice President and Counsel	Credit Suisse Group AG
Melissa	Holds the Enemy		Crow Tribe of Montana
Janet	Wright	Senior Vice President of Corporate, Securities and Finance Counsel and Assistant Secretary	Dell Inc
David	Allgood	Counsel	Dentons Canada LLP
Chantal	Bernier	Counsel Global Privacy and Cybersecurity Group	Dentons Canada LLP

First Name	Last Name	Job Title	Company
Kate	Broer	Partner	Dentons Canada LLP
Marie	McDermott	Global Projects Director	Dentons Canada LLP
Christopher	Pinnington	Canada Chief Executive Officer	Dentons Canada LLP
Katarzyna	Sliwa	Partner	Dentons Canada LLP
Meriam	Al-Rashid	Partner	Dentons US LLP
Joseph	Andrew	Global Chairman	Dentons US LLP
Jana Cohen	Barbe	Global Vice Chair	Dentons US LLP
Meghan	Cocci	Partner	Dentons US LLP
Howard	Dean	Senior Advisor	Dentons US LLP
Elizabeth	Ferrick	Partner	Dentons US LLP
Xeresa Lane	Folsom	Partner	Dentons US LLP
Laura	Gibson	Partner	Dentons US LLP
Susan Poncher	Greenspon	Partner	Dentons US LLP
Jeffrey	Haidet	US Co-Chief Executive Officer	Dentons US LLP
Margaret Donahue	Hall	Partner	Dentons US LLP
Sandra	Hauser	Partner	Dentons US LLP
Mary Ann	Hynes	Senior Counsel	Dentons US LLP
Karen	Jordan	Partner	Dentons US LLP
Heather	Khassian	Counsel	Dentons US LLP
Shari	Klevens	Partner | Deputy General Counsel	Dentons US LLP
Ira	Kotel	Partner	Dentons US LLP
Andi	Mandell	Partner	Dentons US LLP
Dara	Mann	Partner	Dentons US LLP
Stafford	Matthews	Partner	Dentons US LLP
Michael	McNamara	US Managing Partner	Dentons US LLP
Carole	Neville	Partner	Dentons US LLP
Kathleen	O'Connor	Counsel	Dentons US LLP
Rose	Petoskey	Associate	Dentons US LLP
Elliott	Portnoy	Global Chief Executive Officer	Dentons US LLP
Sara Dutschke	Setshwaelo	Counsel	Dentons US LLP
Natalie	Spears	Partner	Dentons US LLP
Toni	Weinstein	Partner	Dentons US LLP
Sandra	Wick Mulvany	Partner	Dentons US LLP
Mary	Wilson	Partner	Dentons US LLP
Peter	Wolfson	US Co-Chief Executive Officer	Dentons US LLP
Deborah	Hoffman	Senior Vice President, General Counsel	Digital Risk LLC

First Name	Last Name	Job Title	Company
Andrea	Giannetta	Vice President and Reinsurance Counsel	Enstar (US) Inc
Mechelle	Evans	Attorney	Essence
Holly	Smith	Assistant General Counsel	Exelon Corporation
Cheryl	Beebe	Board Of Trustees	Fairleigh Dickinson University
Alison	Kutler	Chief of the Consumer and Governmental Affairs Bureau and Special Advisor to the Chairman	Federal Communications Commission
Lisa	Cornehl	Vice President, Deputy General Counsel and Chief Litigation Counsel	First American Financial Corporation
Lynn	Oberlander	General Counsel	First Look Media Inc
Hilary	Gevondyan	Vice President & Associate General Counsel	First Republic Bank
Sherry	Geyer	VP, Associate General Counsel	First Republic Bank
Stacey	Fishbein	Deputy General Counsel	Garden City Group LLC
Stephanie	Westfield	Associate General Counsel	Garden City Group LLC
Nancy	Kumar	Lead Attorney	Georgia Power Company
Kathryn	Weisbeck	Director of Investor Relations	Global Arena Holding Inc.
Katie	Fellows	Vice President and General Counsel	Hard Rock Hotels & Casinos
Amy	King	Vice President and Senior Counsel	Hilton Worldwide Inc
Saundra	Brown-Savoy	Depty General Counsel for Health Sciences	Howard University
Kelli	Keenan	Senior Legal Counsel	HSBC Bank USA NA
Stephanie	Vo	Vice President and Senior Legal Counsel	HSBC Bank USA NA
Ivy	Fischer	Senior Vice President and Chief Legal Counsel	HUB International Northeast Limited
Felicia	Buebel	Assistant General Counsel and Assistant Secretary	Icahn Enterprises LP
Hon. Shira	Sheindlin		JAMS Inc
Alison	Moore	Vice President & Assistant General Counsel	JPMorgan Chase & Co
Deborah	Levine	Vice President and Assistant General Counsel	JPMorgan Chase Bank NA
Janice	Block	Executive Vice President and Chief Legal and Administrative Officer	Kaplan Higher Education Corporation
Yael	Aufgang	Associate General Counsel	Kaplan University
Kim	Stuart	Principal	Key Group
Julie	Cho	Counsel	LAM Group
Bridget	Marsh	Executive Vice President - Deputy General Counsel	Loan Syndication and Trading Association
Paula	Barnes	Senior Counsel	Macy's Inc
Fawn	Horvath	Vice President, Law	Macy's Inc

First Name	Last Name	Job Title	Company
Sonya	Som	Business Development Specialist	Major, Lindsey & Africa
Jacqueline	Keller, Esq.	Head of Legal	Malayan Banking Berhad, New York Branch
Maria	Filipakis		Maria Filipakis
Lorraine	Feldman	Senior Litigation Counsel	Marsh & McLennan Companies Inc
Alexandra	Russello	Litigation Counsel	Marsh & McLennan Companies Inc
Kathleen	Barlow	Senior Vice President	Marsh Inc
Gloria	Santona	Executive Vice President, General Counsel and Secretary	McDonald's Corporation
Margaret	O'Brien	Global Chief Counsel for Health and Benefits	Mercer LLC
Colette	Foster	Corporate Counsel	Metlife Bank NA
Debra	Cohn	General Counsel and Chief Compliance Officer	Metropolitan Council on Jewish Poverty
Theresa	Baker	Assistant General Counsel	Metropolitan Life Insurance Company
Blossom	Kan	Assistant General Counsel	Metropolitan Life Insurance Company
Sheila	Murphy	Senior Vice President and Associate General Counsel	Metropolitan Life Insurance Company
Dennis C.	Garcia	Assistant General Counsel	Microsoft Corporation
Leigh	Weinraub		Mind in Motion
Jennifer	Zimmerman	Executive Director	Morgan Stanley
Cara	Ciuffani	Vice President and Senior Counsel	Morgans Hotel Group
Meredith	Deutsch	Executive Vice President, General Counsel and Corporate Secretary	Morgans Hotel Group
Annemarie	Brennan	V.P. & Assoc. General Counsel	NAM, Sivantos
Lucy	Fato	General Counsel and Managing Director	Nardello & Co. LLP
Darnella	Banks	Corporate Vice President	New York Life
Linda	Beebe	Associate General Counsel	New York Life Insurance Company
Dora	Jimenez	Associate General Counsel	New York Life Insurance Company
Susan	Maisel	Associate General Counsel	New York Life Insurance Company
Priya	Udeshi Crick	Associate General Counsel	New York Life Insurance Company
Maureen	Cronin	Director and Associate General Counsel	New York Life Investment Management LLC
Rachel	Orban	Vice President and Assistant General Counsel	New York Life Investment Management LLC
Rebecca	Strutton	VP and Asst. GC	New York Life Investment Management LLC
Michele	Mayes	Vice President, General Counsel and Secretary	New York Public Library
Eugenie	Gavenchak	Senior Vice President and Deputy General Counsel	News Corp
Cindi	Smith		Nokia Siemens Networks
Mimi	Ton	Senior Legal Counsel	Nokia Siemens Networks

First Name	Last Name	Job Title	Company
Genevieve	Silveroli	Vice President and Corporate Secretary and Head of Legal and Compliance for North America	Nokia Solutions and Networks
Patricia	Ryan	Executive Vice President and General Counsel	Old American Capital Corporation
Cissie	Citardi	Managing Director and Deputy General Counsel	PineBridge Investments
Lauren	Freeman-Bosworth	Vice President, Deputy General Counsel and Litigation	Pitney Bowes Inc
Leda	Moloff	Director of Corporate Counsel	Prudential Financial Inc
Kristina	Dalman	Vice President, Area General Counsel	PulteGroup Inc
Alejandra	Ruiz-Dana		Quiet Lunch
Sue	Chen-Holmes	U.S. Counsel, Executive Director	Rabobank International
Shari	Siegel	Managing Partner & General Counsel	Ranieri Strategies LLC
Tracy	Edwards	Tribal Chief Executive Officer and Outgoing Tribal Chairperson	Redding Rancheria
Julia	Herr	General Counsel	Redwood Capital Management, LLC
Denise	Turner-Walsh	In House Counsel	Rincon Band of Luiseno Indians
Dominique	Charles	Contract Attorney	Roosevelt Management Company LLC
Jessica	Smith	Assistant General Counsel	Roosevelt Management Company LLC
Inna	Zumor	Assistant General Counsel and Compliance Officer	SAM LLC
Marianne	Hill	Acting Vice President for Legal and Prime Contract, Acting General Counsel, and Corporate Secretary	Sandia National Laboratories
Teresa	Cappella	Senior Vice President, General Counsel	Shenkman Capital Management, Inc.
Leslie	Kirk	General Counsel	Siebert Brandford Shank a co., L.L.C.
Kwarma	Vanderpuye	Senior Vice President, General Counsel	SmithDehn India
Leigh	Davis		Southern Company
Laura	Hewett	Associate General Counsel	Southern Company Services, Inc.
Catherine	Nathan	Partner and Former Co-Head	Spencer Stuart
Lauren	Tanen	Director of Legal Employment Law	Spotify
Ilona	Korzha	Counsel	Sprint Nextel Corporation
Nadine	Greenwood	Senior Vice President and and Associate General Counsel	Starwood Hotels & Resorts Worldwide Inc
Laura	Mutterperl	Vice President, Associate General Counsel	Starwood Hotels & Resorts Worldwide Inc
Kristen	Prohl	Chief Regulatory Counsel	Starwood Hotels & Resorts Worldwide Inc
Ainslee	Schreiber	Vice President and Associate General Counsel	Starwood Hotels & Resorts Worldwide Inc
Rachel	Schatten	General Counsel and Chief Compliance Officer	StoneCastle Partners, LLC

First Name	Last Name	Job Title	Company
Betsy	Kamin		Strasburger & Price LLP
Melissa	Kennedy	Executive Vice President and General Counsel	Sun Life Assurance Company of Canada
Aparna	Williams		Symantec Corporation
Susan	Donnellan	Director and Associate General Counsel	Teachers Insurance and Annuity Association - College Retirement Equities Fund
Christa	Rapoport	Senior Vice President	The Goldwater Taplin Group
Sloane	Perras	Chief Legal Officer	The Krystal Company & On The Border Mexican Grill & Cantina
Julie	Bowen	Vice President, General Counsel and Corporate Secretary	The MITRE Corporation
Mychal	Boyd	Senior Counsel	The Travelers Companies Inc
Kim	Dionne		The Travelers Indemnity Company
Ann	Mulcahy	Executive Counsel	The Travelers Indemnity Company
Dina	Traugot	Vice President	The Travelers Indemnity Company
Karen	Lorenzo	General Counsel	Tribeca Enterprises
Cheryle	Bernard-Shaw	Chief Compliance Officer	Tri-City Healthcare District
Jennifer	Kraft	Deputy General Counsel and Corporate Secretary	United Continental Holdings Inc
Jenn	Silver	Inhouse Counsel	Viacom Inc
Sheri	Dethlefs	Senior Director, Business Affairs and Secretary	Wazee Digital, Inc.
Christina	Ibrahim	Executive Vice President and General Counsel and Corporate Secretary	Weatherford International Inc
Jean	Kim	Senior Counsel	Wells Fargo Bank NA
Kimberlee	Yapchai	Senior Director	Whirlpool Corporation
Deidra	Gold	Executive Vice President and General Counsel	Wolters Kluwer Health Inc
Suzan	Friedberg	Associate General Counsel, Claims Legal	XL Catlin Insurance
Megan	Belcher		
Maureen	Brundage	Governance and Securities Law Expert	
Izumi	Fukushima		
Ignacia	Moreno		

Tab 4

Navigating Cybersecurity in a Global Economy

Chantal Bernier, Counsel, Dentons

Dennis Garcia, Assistant General Counsel, Microsoft

Aparna Williams, Director of Global Selling Programs and Channels, Legal and Public Affairs, Symantec Corporation

Strong winds, best tacks

- New Governance for New Challenges
- Assessing Risk Globally
- Optimizing Cloud Use
- Managing the Human Factor
- Dealing with an Evolving Regulatory Landscape
- Responding to Breach

New governance for new challenges

5 Golden Rules of Accountability

1. The Board must be engaged as a matter of corporate risk
2. The CEO cannot pass the buck, anymore than for profitability
3. The CPO and the CIO must work hand in glove for effectiveness
4. Each manager must ensure compliance as a matter of performance
5. Each employee must endorse cybersecurity as a matter of ethics

Governance structure

Who is responsible for Cybersecurity?

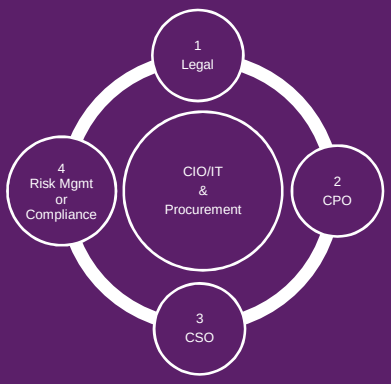
- Board of Directors?
- Risk/Insurance?
- Global Security Office /IT?
- Privacy Office?
- Legal?

Assessing Risk Globally

Assessing Global Risk

- Connected to the Internet – You Have Risk!
- How do you quantify that risk?
  - Infrastructure
  - Applications
  - People
- Strategy for mitigating risk
- Are you insurable against these risks?

Assemble & Engage Your Team



@DennisCGarcia

Microsoft

Security

- Technical & operational
- Physical security
- Threat management teams
- Strong data encryption
- Fighting cybercrime

@DennisCGarcia

Microsoft

Privacy & Control

- Data processing terms & EU Model Clauses
- Privacy regulator validation
- Positive history with regulators
- Options: Cloud AND On-Premises
- Customer owns its data
- Limited data usage by cloud provider
- Third party requests for data wording
- Sues others to protect your data
- Seeks to modernize data laws

@DennisCGarcia

Microsoft

Comply

Microsoft cloud services have the largest compliance portfolio in the industry

@DennisCGarcia

Microsoft

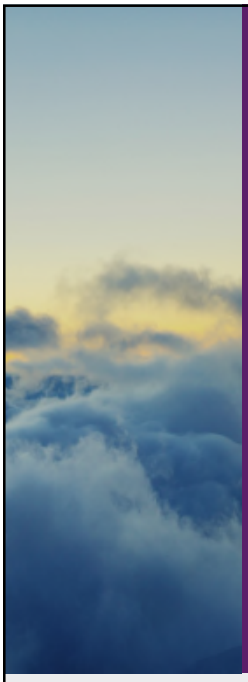
Optimizing Cloud

Goal: Find a Trusted Cloud/IT Provider

Companies will only use technology they trust

@DennisCGarcia

Microsoft



Inspiring Trust in the Cloud

Security
Committed to the protection of your data in cloud services

Privacy & Control
Maintain privacy and control of your data when using cloud services

Comply
Meet your compliance needs when using cloud services

Transparency
Understand what happens with your data in cloud services

@DennisCGarcia

Microsoft

Cloud and Third Party Service Providers

Who do you trust to secure your systems and data?

- What are you putting into the cloud?
- How difficult would it be if that data were lost?
- How much damage would occur if the data were leaked?
- Do you understand the meaning of built to fail? Failover capacity? Failover across borders?

Transparency

- Microsoft Trust Center
- Microsoft Transparency Hub
- Law Enforcement Requests Reports
- Data location specificity
- Identity of subcontractors
- Easy access to audit reports
- Clear cloud contract provisions
- No contract changes for contract term
- Data center tours

@DennisCGarcia

Microsoft

Managing the Human Factor

How weak is the weakest link…

- 78% of breaches have employee negligence at their root cause
- Employees either:
  - Lack digital literacy
  - Snoop
  - Steal
- And it is expensive:
  - $400M in class action against Rouge Valley for employee snooping
  - $ 5M$ in class action against Scotia Bank for employee unauthorized use

Increase Digital Literacy

The Human Factor

- Human error accounts for the majority of weaknesses in a system
- Ongoing training, reminders and tests are good tools
- Do you use appropriate level of login and password checks?
- How is your physical security?
- How is your technological security?
  - Can someone cut into a wall and log into your network?
  - Are you sure?

Dealing with an Evolving Regulatory Landscape

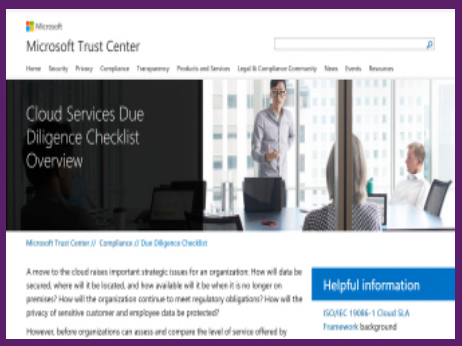
It’s hoppin’

- October 6, 2015 : Invalidation of Safe Harbour
- July 12, 2016 : Privacy Shield is deemed adequate
- April 27, 2016 : adoption of General Data Protection Regulation (GDPR) to come into force May 25, 2018
- September 15, 2016: ISO 19086 is published
- November 10, 2016: Linkedin is blocked in Russia on the basis of data residency requirements
- Data residency requirements are proliferating globally

Evolving Regulatory Landscape

- Governments are looking into using cloud and are focusing on cybersecurity as a priority
- Governments are setting standards and metrics for cybersecurity
  - Are they global / scalable?
- Creating a criminal code for cyber attacks can become challenging
  - How do you prosecute?

ISO 19086



@DennisCGarcia

Microsoft

Territorial scope of access to data

- *Microsoft vs United States* (Ireland case)
- *Law Enforcement Access to Data Stored Abroad Act (LEAD ACT)*
- Territorial Scope of the GDPR

Responding to an Event

Some basic reminders…

- This is not the time to improvise
- CYA is not a recognized ethical principle
- The test is no longer occurrence but accountability

Responding to an Event

- Do you have an information classification plan / standard?
- Do you know where your data resides?
  - The sensitive data and the not-so-sensitive?
- Are you certain that your security measures are adequate?
- Do you know the requirements around securing data?
- Do you have a situation-room / plan to address an event?

Navigational Warnings and Beacons

- Knowledge of Domestic Law is no Longer Enough
  - Get your global legal network in place
- Cloud is the way of the future
  - Learn the risks and exercise due diligence
- Your biggest threat is inside
  - Get the appropriate safeguards in place
- Cybersecurity is a corporate risk
  - Address it corporately
- A breach is not the time to improvise
  - Have your breach response plan ready and tested

Boards' Oversight for Privacy

Chantal Bernier, Counsel, Dentons LLP Canada, former Interim Privacy Commissioner of Canada.

It's about knowing the right questions

Throughout my experience chairing a board or being a board member, the same underlying question constantly resurfaces: when is the board fully exercising its oversight function and when is it encroaching upon management of the organization? In relation to privacy, in the wake of spectacular breaches (Target, Anthem, Sony or the Carbanak attack, which siphoned millions from 100 banks), the business world has been rocked by the magnitude of this new liability and, therefore, by the realization of boards' duty of care in this regard.

This article seeks to explore best practices for boards to oversee corporate management of privacy and data security. It first addresses the legal groundings for the role of boards, then moving to corporate obligations for protection of personal information, and finally draws some guidance for board members to ask the right questions of senior management and for senior management to provide the right answers.

The Grounding: Agreeing on a Definition of Boards' Scope of Oversight Function

As the issue is universal, I will turn to the eloquent remarks of Luis Aguilar, Commissioner of the United States Securities and Exchange Commission, on the role of boards specifically with regard to protection of personal information or, as personal information is now held in cyberspace, to cyber security:

> When considering the board's role in addressing cybersecurity issues, it is useful to keep in mind the broad duties that the board owes to the corporation and, more specifically the board's role in corporate governance and overseeing risk management. It has long been the accepted model, both here and around the world, that corporations are managed under the direction of their boards of directors. This model arises from a central tenet of the modern corporation — the separation of ownership and control of the corporation. Under this structure, those who manage a corporation must answer to the true owners of the company — the shareholders.[1]

Perhaps less eloquent but clarifying the state of the law, the decision of the Supreme Court of Canada in *Peoples Department Stores v. Wise* outlines two duties of a board:

> [The first] duty requires directors and officers to act honestly and in good faith with a view to the best interests of the corporation. The second duty is commonly referred to as the "duty of care". Generally speaking, it imposes a legal obligation upon directors and officers to be diligent in supervising and managing the corporation's affairs.[2]

---

[1] Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Cyber-Risks and the Boardroom Conference, New York, June 19, 2014, http:///www.sec.gov/News/Speech/Detail/Speech/13705 42057946.
[2] *Peoples Department Stores Inc. v. Wise*, 2004 SCC 68 at paragraph 32. See *Canada Business Corporations Act*, R.S.C. 1985, c. C-44, s. 122(1):

The scope of "duty of care" in relation to privacy is therefore determined by the obligations of the company in this respect.

Corporate Privacy Obligations

In typical Canadian fashion, privacy protection in the private sector in Canada is governed by a mix of federal and provincial legislation. In short:

- Commercial activity by organizations coming under federal jurisdiction (airlines, banks, for example) in all of Canada is governed by the federal Personal Information Protection and Electronic Documents Act ("PIPEDA").[3]
- Commercial activity by any organization under provincial jurisdiction is governed by PIPEDA, except in British Columbia, Alberta and Quebec, which have their own private sector privacy legislation.[4]
- Commercial activity in the health sector is governed by provincial legislation in eight provinces.[5] These include Ontario,[6] New Brunswick,[7] Nova Scotia,[8] Saskatchewan,[9] Manitoba,[10] Alberta,[11] Prince Edward Island[12] and Newfoundland and Labrador.[13]

The common thread underlying the privacy protection regime in Canada is found in the Model Code for the Protection of Personal Information.[14] The regime rests upon 10 principles that should form the matrix for boards' oversight of privacy protection, including cyber security.

> *Principle 1: Accountability*. An organization is responsible for the personal information in its custody. This requires that the organization: (i) designate an individual responsible for the "day-to-day collection and processing of personal information;" (ii) make the identity of this individual available upon request; (iii) implement policies and practices to

---

> 122. (1) Every director and officer of a corporation in exercising their powers and discharging their duties shall:
> (a) act honestly and in good faith with a view to the best interests of the corporation; and
> (b) exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances.

[3] *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), S.C. 2000, c. 5.
[4] *British Columbia, Personal Information Protection Act*, S.B.C. 2003, c. 63; Alberta, *Personal Information Protection Act*, S.A. 2003, c. P-6.5; Quebec, *Act respecting the protection of personal information in the private sector*, C.Q.L.R. c. P-39.1.
[5] However, only Ontario, New Brunswick and Newfoundland and Labrador have health information privacy legislation that has been declared substantially similar to PIPEDA with respect to health information custodians. While other provinces and territories have also passed their own health privacy laws, these have not been declared substantially similar to PIPEDA. Therefore, in some cases, PIPEDA may still apply. "Fact Sheets: Privacy Legislation in Canada," Office of the Privacy Commissioner, May 2014.
[6] *Ontario Personal Health Information Protection Act*, S.O. 2004, c. 3, Sched. A.
[7] New Brunswick *Personal Health Information Privacy and Access Act*, S.N.B. 2009, c. P-7.05.
[8] Nova Scotia *Personal Health Information Act*, S.N.S. 2010, c. 41.
[9] Saskatchewan *Health Information Protection Act*, 2009, c. H0.021.
[10] Manitoba *Personal Health Information* Act, C.C.S.M. c. P33.5.
[11] Alberta *Health Information Act*, R.S.A. 2000, c. H-5.
[12] Prince Edward Island *Health Information Act*, Bill No. 42, 4th Session, 64th General Assembly. Received Royal Assent May 14, 2014, not yet in effect.
[13] Newfoundland and Labrador *Personal Health Information Act*, SNL 2008, c. P-7.01.
[14] CAN/CSA-Q830-96, Schedule 1, PIPEDA.

> protect personal information; (iv) establish procedures to receive and respond to com-plaints and inquiries; and (v) train staff on the policies and practices as well as developing information to explain them.[15]

A concrete example of the importance of establishing a governance framework is found in the Office of the Privacy Commissioner of Canada ("OPC") Report of Findings of 2011 on Google Wi-Fi.[16] In a nutshell, the investigation revealed that a Google engineer, on his own initiative, developed a code capable of sampling categories of publicly broadcast Wi-Fi data. It was introduced in the Street View program without verification of its actual functions or privacy impact. As a result, Google found itself unlawfully collecting payload data, or content of communications. Twelve countries investigated Google, all coming to the conclusion of significant governance failures.

The case of Google Wi-Fi brings to light the importance of compliance with the Accountability Principle and lays at the feet of the board the duty to oversee it. That is board business: ensuring the organization has the governance structures to fulfill its obligations.

A crucial point about accountability is that an organization remains "responsible for the information in its possession or custody, including where that has been transferred to a third party for processing." This applies to transfers both within Canada and abroad and subjects such transfers to stringent contractual clauses whereby the organization ensures a level of protection equivalent to that in Canada and mechanisms for verification.

Boards should inquire about the integration of privacy protection in outsourcing contracts that entail transfer of personal information, in Canada and outside, with even greater insistence if the information is transferred to a third party located in a country with weak or non-existent privacy laws.

> *Principle 2: Identifying purposes*. Upon collection of information, an organization must clearly identify the purposes for collection, and collection must be limited to what is necessary for those purposes. Where the information is meant to be used for another purpose than the ones identified upon collection, new consent is required.[17]

The specific application of this principle has caused some controversy lately in the Report of Findings of the OPC with respect to Bell Canada's Relevant Ads Program.[18] The issue at hand is this: is the use of personal information for interest-based advertising a purpose distinct from the purpose of collection, namely to provide Bell service? The disputed conclusion of the OPC was that indeed it is a different purpose and is therefore subject to consent. Moreover, the OPC concluded that it is subject to express consent, on the basis of two factors: (i) because the ads were delivered on the basis of a compilation of numerous pieces of personal information, including credit information, constituting a profile of the customer, the personal information was sensitive information; and (ii) because users had already paid for the service, the OPC concluded that they had a high expectation that their personal information would not be used to serve ads.

The board's interest in such a matter is illustrated by the cost both in corporate image (within two weeks, the OPC had received nearly 200 complaints with respect to Bell Canada before I decided to initiate an investigation) as well as in legal costs and operational costs, such as abandoning a program after it has been rolled out. The impact on organizations

---

[15] PIPEDA, supra note 3, Schedule 1, 4.1.
[16] "Report of Findings: Google Inc. WiFi Data Collection," PIPEDA Report of Findings #2011-001, online: https://www.priv.gc.ca/cf-dc/2011/2011_001_05 20_e.asp.
[17] PIPEDA, supra note 3, Schedule 1, 4.2.1.
[18] Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program," PIPEDA Report of Finding #2015-001, online: https://www.priv.gc.ca/cf-dc/2015/2015_001_0407_e. asp.

certainly begs, in my view, for presentation of the program to the board prior to rolling it out for the board to inquire about privacy implications and assess the risk to the company.

> *Principle 3: Consent*. In private sector privacy law, the notion of consent is pivotal. It is not an "Open Sesame" but it is the gateway to collect, use or disclose personal information lawfully. The condition is that it must be meaningful consent, namely informed with relevant knowledge and based on a description of the purposes "in a manner that the individual can reasonably understand how the information will be used or disclosed."[19] A tricky limitation in the context of Internet service based on advertisement using personal information is that "(a)n organization shall not, as a condition of service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes."[20]

The specific issue of consent as a condition of service first came up in relation to new business models online and specifically in the context of advertising. In 2009, the OPC investigation into Facebook[21] stated that this privacy principle had to be applied taking into account the reality of a free service that could not be offered without advertising. The consequence is that the user should expect advertising in these circumstances but with the restriction that it could not be overly intrusive (such as Facebook social ads, which used users' actions, thumbnail photos and names to promote products) and that the personal information guiding the targeting of the ads could not be disclosed to third parties. This same reasoning underpins the findings with respect to Bell: drawing a profile of the user was considered overly intrusive and since the information was not provided in the context of a free service, the users' expectation of privacy was deemed too high to allow interest-based advertising without consent.

Again, the complexity of these distinctions calls for full briefing of the board with an assessment of privacy risks and mitigation strategies when a product that has privacy implications gets rolled out. Too much is at stake not to.

> *Principle 4: Limiting collection*. As mentioned regarding Principle 2, collection of personal information must be limited to what is necessary to fulfill the purpose identified by the organization. Section 5(3) of PIPEDA further narrows the limitation to allow collection "only for purposes that a reasonable person would consider are appropriate in the circumstances."

Examples abound from privacy investigations on the necessity and appropriateness of organizations requiring specific information. The rule that emerges can be summarized as this: if the collection of the information can be justified as relevant to deliver the service, it is appropriate to collect it.

In relation to board oversight, the question would be to ensure that the organization does not collect personal information without consent beyond what is relevant to deliver service. The board does not second-guess management but must require a cogent case to buttress data collection.

> ·*Principle 5. The limitation of use, disclosure and retention*. In relation to use, information cannot be used for a purpose different than the one for which the information was collected; in relation to disclosure, organizations cannot disclose information without consent except as required by law; in relation to retention, organizations must "develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods."

---

[19] PIPEDA, supra note 3, Schedule 1, 4.3.2.
[20] Ibid. Schedule 1, 4.3.3.
[21] "Report of Findings into the Complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act," PIPEDA Case Summary #2009-008, online: https:// www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp.

Obligations relating to retention particularly come within the ambit of the board since they relate to governance. They require a policy for a retention schedule, based on relevant legal requirements, fulfillment of the individual's right of access to the personal information and disposal when it has become irrelevant. Retention schedules are central to information management plans and boards should inquire as to their existence and justification.

> *Principle 6: Accuracy*. This may be the principle of least interest to boards since it pertains squarely to operations. Essentially, organizations have the obligation to keep personal information "accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."[22]
>
> *Principle 7: Safeguards*. This is where the rubber meets the road, where Target lost its CEO and Sony its Chairperson of the Motion Picture Group of Sony Pictures Entertainment. It is also where 100 banks lost an estimated $1 billion to the Carbanak hackers. The liability is such to unquestionably trigger boards' obligations of due diligence. Canadian law describes obligations under the principle of safeguards as the obligation to adopt "security safeguards appropriate to the sensitivity of the information."[23] The methods of protection must include:
>
> (a) physical measures such as locked cabinets and secure areas;
>
> (b) organizational measures, such as policies and processes to control access to information, issuing a clear retention schedule and performing threat and risk assessments to develop mitigating measures; and
>
> (c) technological measures such as encryption, passwords and audit trails.

In the speech referred to earlier in this article, Commissioner Aguilar has some concrete recommendations for boards in this area:

- As a first step, boards should work with management to assess their corporate practices against cyber security standards. Commissioner Aguilar refers to the National Institute of Standards and Technology's Cybersecurity Framework,[24] but there is excellent guidance in Canada as well. For example, Public Safety Canada has issued "Get Cyber Safe Guide for Small and Medium Businesses"[25] and Ray Boisvert has published "What every CEO needs to know about cybersecurity: A background paper," which serves as a tool to guide the board in ensuring accountability for safeguards.[26]
- Boards also need to ensure they have the technical expertise to "evaluate whether management is taking appropriate steps to address cybersecurity issues."[27] This can be achieved by ensuring that this skills set is represented on the board, creating a specific committee of the board on cyber security risk management, or providing the board with cyber-risk education.

---

[22] PIPEDA, supra note 3, Schedule 1, 4.7.
[23] Ibid., Schedule 1, 4.6.
[24] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, February 12, 2014, online: http://www. nist.gov/cyberframework/upload/cybersecurity-frame work-021214.pdf.
[25] www.GetCyberSafe.gc.ca
[26] Ray Boisvert, "What every CEO needs to know about cybersecurity," Online: http://www.continue.uottawa.ca/uploads/File/What-Every-CEO-Must-Know-Cyber-April -4-2014-Fin al.pdf.
[27] Speech by Commissioner Luis Aguilar, supra note 1.

- Exercising due diligence in relation to security also entails the need for boards to understand the company's cyber security governance framework: knowing who is responsible for risk oversight and for ensuring the adequacy of risk management.

- Importantly, boards should ensure that management has developed a "well-constructed and deliberate" breach response plan consistent with industry standards.

In relation to safeguards, as with all other corporate issues, the board must fulfill its role to direct and protect by holding management accountable for minimizing risk. The added challenge is that safeguards now rest upon a complex ecosystem of physical, technological and administrative measures that are a challenge to master and yet pose heightened risk. Hence, the urgency for boards to address gaps in knowledge and in awareness in that regard.

> *Principle 8: Openness*. An organization must make readily available its policies and practices relating to the management of personal information. Specifically, information must be made available without unreasonable effort and the information made available must include the name of the person responsible for complaints or inquiries to the organization.

Where this compliance principle comes within the ambit of the board is where it defines an organization's transparency in relation to its collection, use, retention and disclosure of personal information. A case in point is the 2014 Report of Findings of the Office of the Privacy Commissioner of Canada regarding Apple.[28] In investigating a complaint alleging excessive collection of information, the OPC found that the collection was justified but that Apple's "privacy policy did not fully identify the purposes for which it collects personal information from users." After Apple agreed to revise its privacy policy to be more open, the complaint was found to be conditionally resolved, pending implementation of the recommendations of the OPC.

The oversight of the board in relation to transparency is made easier, in my view, with the "Ten Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency" issued by the OPC.[29]

> *Principle 9: Individual access.* Part of the fundamental right to privacy is the right to know what others know about you. Consequently, individuals about whom an organization holds personal information have the right to obtain access to that information. Moreover, the individual has the right to challenge the completeness and accuracy of the information. The exceptions to that principle are where: (i) it is prohibitively costly to provide the information; (ii) the information includes information about others; (iii) the information may not be disclosed for legal, security or commercial proprietary reasons; or (iv) the information is subject to litigation privilege.

The principle relates more to the operations of information management than to policy strategy and therefore, should not normally come within the ambit of the board. The exception would be if the organization egregiously fails in this regard, either by systemic denial of access or by abuse of power, in which case the risk for litigation must be brought to the board and the board may ask, in exercising due diligence, for statistics on access requests to assess compliance.

> *Principle 10: Challenging compliance*. In contrast to Principle 9, Principle 10 definitely comes within the scope of board oversight since it is a pillar of sound governance. All organizations holding personal information must provide

---

[28] "Apple called upon to be more open about its collection and use of information for downloads," PIPEDA Case Summary #2014-007, online: https:// www.priv.gc.ca/cf-dc/2014/2014_007_1010_e.asp.
[29] "Fact Sheets: Ten Tips for a better Online Privacy Policy and Improved Privacy Practice Transparency," Office of the Privacy Commissioner of Canada, online: https://www.priv.gc.ca/resource/fs-fi/02_05_d_56_tips 2_e.asp.

> means to challenge its compliance with privacy obligations through procedures to receive and respond to complaints that are "easily accessible and simple to use."[30]

In reviewing the organization's exposure to privacy risks, the board must simply ascertain that proper recourse mechanisms exist for users or customers to exercise their rights in relation to the protection and accuracy of the personal information the organization holds about them.

Conclusion: Knowing the Right Questions

In *The Imperfect Board Member*,[31] Jim Brown summarizes in an effective, if not scientific, way the scope of a board's duty of care: "The best boards keep their noses in the business and their fingers out."" This one degree of separation between management and board is where management should know the right answers and the board should know the right questions. That is the raison d'être of boards: creating a forum for asking the questions that will assess the quality of management in relation to the objectives and obligations of the organization.

Until now, my observation from seeing so many companies from the inside yields the conclusion that in relation to privacy oversight, boards are mainly hampered by three main gaps: (i) lack of awareness of their responsibility to oversee privacy protection, (ii) excessive delegation to technologists as if it were a mere technological issue rather than part of a strategic ecosystem of protection of personal information; and (iii) insufficient technical expertise to assess protection of personal information, particularly in relation to cyber security.

In fairness, companies' awareness is indisputably rising as a result of the spectacular breaches that have affected them or their competitors, boards are gradually reclaiming their role in challenging information management strategies and technical knowledge is broadening. I would like to see further changes:

- Privacy, not merely data protection, must be the focus of board oversight. This means showing a concern that goes beyond the mere security of data. It must include an approach that protects individuals from unjustified intrusion.

- Privacy must be seen for what it is: a fundamental right and a visceral need. The number of complaints to regulators, class actions and walking away from companies having suffered a breach certainly demonstrate individuals' attachment to that sacred space we call privacy. The matter therefore comes within the ambit of the board as a matter of integrity of the organization, in addition to competitiveness and risk management, as central to the success of the organization as financial management.

- Boards must assess the strength of governance structures within the organization to ascertain it can demonstrate compliance with privacy obligations. I may be biased since I co-led its development, but that admitted, I believe the guide "Getting Accountability Right with a Privacy Management Program" can provide useful guidance to boards in holding management accountable in that regard."

---

[30] PIPEDA, supra note 3, Schedule 1, 4.10.2.
[31] Ibid. at 88.

- Boards should increase their knowledge and understanding of privacy obligations and information technology properties, enough to know the right questions to ask.[32]

Considering what is at stake, for organizations and for individuals, in the event of a failure in protecting privacy, the board's duty to direct and protect necessarily takes us to an increased focus on directing the organization to respect privacy, in order to protect its interests and integrity.

Chantal Bernier, Counsel,
Dentons LLP Canada
+1 613 783-9684
chantal.bernier@dentons.com

[32] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner of British Columbia, https://www.priv.gc.ca/information/guide/2012/gLacc_201204_e_asp.

dentons.com

大成 DENTONS

Privacy and security guidance

Cloud computing in the MUSH Sector

Operational privacy risks and opportunities in cloud computing: a focus on municipalities, universities, school boards, and hospitals (MUSH sector)

Table of contents:

Purpose of this guidance document and how to apply

This document is intended to be used by decision makers in the MUSH sector when considering using cloud services.

The document compiles observations and recommendations from a roundtable discussion held on June 16, 2015.

The discussion was based on a preliminary document on cloud computing for the MUSH sector prepared by Dentons Canada LLP. Operational advice was provided by experts from academic, medical, government, and private institutions.

Why focus on the MUSH sector?

Cloud computing is attractive to any organization holding personal information with limited means to secure it. Ensuring privacy and security is a particular challenge for organizations in the MUSH sector. To provide essential services, they must collect and hold highly sensitive data, yet they have limited resources to protect it. Not surprisingly, these organizations appear to be increasingly vulnerable to information security breaches[1].

[1] See Anna Wilde Mathews & Danny Yadron, 'Health Insurer Anthem Hit by Hackers', Wall Street Journal, 4 February 2015; Natasha Singer, 'Uncovering Security Flaws in Digital Education Products for Schoolchildren', The New York Times, 8 February 2015.

Examples of identified operational cloud risks and benefits in health care institutions

Benefits

Simplification of information management;

Reducing costs in IT staff

Scalable infrastructure;

Tiered data storage;

Remote disaster recovery and business continuity;

Facilitated collaboration;

Continuity of patient care;

Easy and rapid access;

Comprehensive report generation;

Harmonization of information standards, enhanced control and security measures; and

Increased patient care quality.

Risks

Breaches through information sharing;

Data leakage in multiple tenancy clouds; and

Loss of control on data through de-localization and remoteness.

Examples of identified operational cloud risks and benefits in educational institutions

Benefits

Reducing costs in IT staff, software and infrastructure;

Increasing data security;

Meeting students' expectations with increased access to new technologies;

Facilitating content sharing and collaboration;

Offering world-wide access.

Risks

Security weaknesses (e.g. passwords in clear text, non-encryption) in relation to e-books, Massive Open Online Courses (MOOC), student or parent-teacher email exchanges;

Data analytics and online behavioural advertising based on sensitive information from databases (identifiers, marks, comments) and individualized teaching;

Cyber-bullying, unwanted contacts, ID theft; Excessive collection and retention of sensitive data; and

Inadequate safeguards in relation to vulnerability and life experience of users.

What is cloud computing?

The National Institute of Standards and Technology of the United States Department of Commerce ('NIST') defines cloud computing as ubiquitous access to a shared pool of configurable computing resources.[2] These resources could be networks, servers, storage, applications, or services. Below are five characteristics of cloud computing. include:

Characteristics of cloud computing

On-demand self-service	A consumer can access the computing capabilities whenever and wherever they wish.
Broad network access	Computing capabilities are delivered over a private network or the internet.
Resource pooling	The provider's computing resources are pooled to serve many consumers.
Rapid elasticity	Computing capabilities can be scaled according to consumer demand.
Measured Service	Consumers can pay for service on a pay-per-use or pay-as-you-go basis.

2 This section benefited from information provided by NIST, the United Kingdom Information Commissioner's Office ('ICO'), and the Office of the Privacy Commissioner of Canada (OPC). See Peter Mell & Timothy Grance, NIST Special Publication 800-145 'The NIST Definition of Cloud Computing', September 2011, online: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; 'Guidance on the use of cloud computing', UK ICO, 2012, online: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf; 'Fact Sheets: Cloud Computing', Office of the Privacy Commissioner of Canada,4 October 2011, online: https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_02_e.asp .

Services models

Software as a Service (SaaS)

Consumers may use the provider's applications running on cloud infrastructure (for example, web-based email or customer relationship management software).

Platform as a Service (PaaS)

Consumers may write or run applications on a cloud-provided platform (for example, a social networking service may offer a platform for software developers to create applications which may utilize data and provide functionality for users of the social networking service).

Infrastructure as a Service (IaaS)

Consumers may access raw computing resources of a cloud service according to the capacity required (for example, a software developer may test an application in a simulated environment on a cloud service before transferring the software to a live environment).

Deployment models

Public cloud

In the public cloud, the cloud services are available to the general public over the internet, while the infrastructure, platform, or software is managed by the cloud provider.

Private cloud

In the private cloud, the consumer is the exclusive user of the service.

Community cloud

In the community cloud, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider.

Hybrid cloud

In the hybrid cloud, the cloud infrastructure is composed of two or more cloud infrastructures that remain unique.

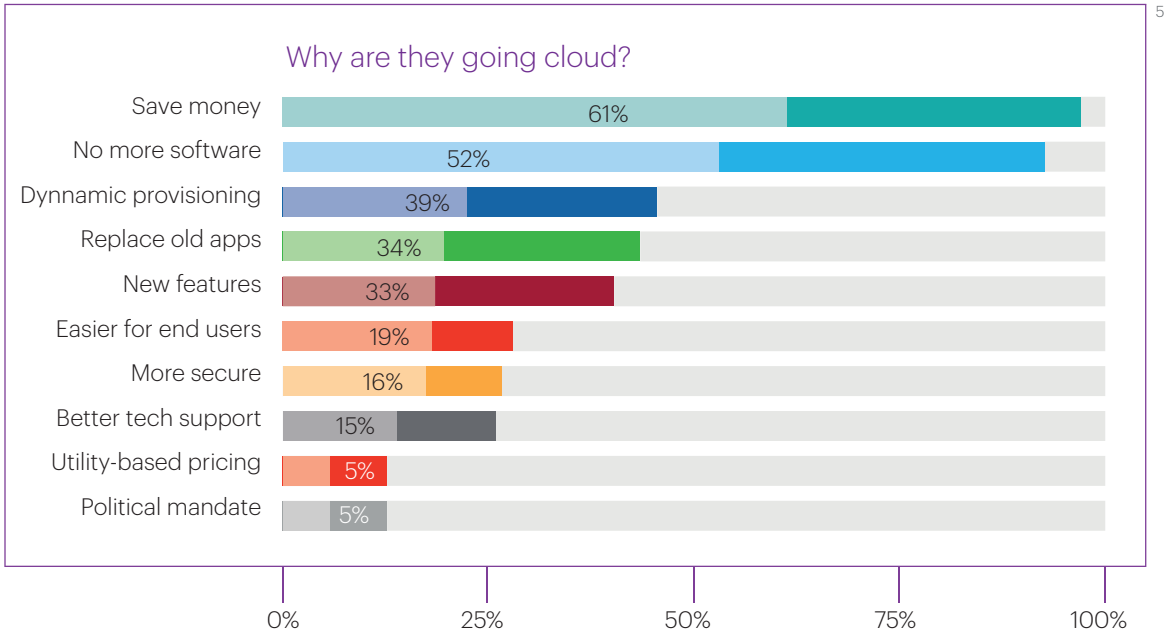
Why use the cloud?

The Office of the Privacy Commissioner of Canada identifies the main benefits of cloud computing as:

- Scalability, by offering unlimited storage and processing capacity;
- Reliability, since it eliminates the risk of losing paper, laptops, or hard drives and allows access to documents and applications via the Internet worldwide;
- Cost savings, since resources are pooled for optimal safeguards thus eliminating the need for investment in infrastructure;
- Efficiency, as the freeing-up of resources through the pooling of expertise allows focus on other priorities; and
- Access to new technology as the cloud providers, being more resourceful and specialized in the area, are in a position to offer a much broader choice.[3]

The Québec Commission d'accès à l'information adds: increased storage capacity and opportunity to base expenses on actual use. Experts underline the low cost of cloud computing and world wide availability.[4]

A survey conducted by SafeGov indicated why many organizations are 'going cloud':



[5]

3 'Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing', Office of the Privacy Commissioner of Canada, May 2010, online: https://www.priv.gc.ca/resource/consultations/report_201105_e.pdf.

4 Martin PJ Kratz, Canada's Internet Law in a Nutshell (Carswell, 2013), at 488; 'Privacy in Cloud Computing', ITU-T Technology Watch Report, March 2012, online: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf.

5 Chart 3, "Survey on Cloud Computing and Law Enforcement", The International Association of Chiefs of Police (IACP), the Ponemon Institute, and SafeGov, January 2013, online: http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=2892&issue_id=32013.

Due diligence on the cloud

When considering whether to move to cloud computing, MUSH organizations should exercise due diligence commensurate to the sensitivity of the personal information they hold by:

1. Assessing organizational needs and available cloud computing services;
2. Examining legal obligations in relation to privacy protection;
3. Performing a risk/benefit analysis of cloud computing in relation to their particular mandate; and
4. Negotiating with the cloud provider,

    - Appropriate authentication/access controls that correspond with the sensitivity of the data;
    - Business continuity measures to prevent data loss in case of an outage, particularly if essential services are provided;
    - Capacity to integrate existing directory services, considering the number of files on one individual, as well as the fact that some files may go on cloud and others not;
    - Financial stability, technological security, track record and corporate responsibility, to ensure long-term service, considering the essential, long-term mandates of MUSH organizations;
    - Clear policies for cookies, data collection minimization, use, retention and disclosure, and individual access rights;

    - Protocol for managing encryption;
    - Termination clauses to recover or delete all personal information held in the cloud;
    - Plan for data breach response;
    - Breach insurance or indemnification;
    - Transparent policies about purposes of cloud out-sourcing and in obtaining consent, considering the sensitivity of data collected in the MUSH Sector;
    - Describing each party's obligations; and
    - Providing for periodic audits.

The clauses are essential and yet may be difficult to secure. Many MUSH institutions find themselves in front of "take it or leave it" cloud computing contracts. A solution is to go with a cloud provider compliant with ISO/IEC 27018 Code of Practice for Personally Identifiably Information ('PII') Protection in Public Clouds Acting as PII Processors which requires all these guarantees as a matter of certification.[6]

6 Based on ISO/IEC 27018 and guidance from the following documents: 'Department Releases New Guidance on Protecting Student Privacy While Using Online Educational Services', US Department of Education, 25 February 2014, online: http://www.ed.gov/news/press-releases/department-releases-new-guidance-protecting-student-privacy-while-using-online-educational-services.

Wayne Jansen & Timothy Grance, 'Guidelines on Security and Privacy in Public Cloud Computing' Special Publication 800-144, US Department of Commerce National Institute of Standards and Technology, December 2011, online: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

See Jeffrey White, 'Cloud Computing in Healthcare: Is there a Silver Lining?', Aspen Advisors, December 2010, online: http://www.aspenadvisors.net/results/whitepaper/cloud-computing-healthcare-there-silver-lining; 'Cloud Computing for Health Care Organizations', Foley & Lardner LLP Health Care Industry Team and IT & Outsourcing Practice, 26 November 2012, online: http://www.foley.com/cloud-computing-for-health-care-organizations-11-26-2012/.

ISO/IEC 27018 standard for privacy on the cloud

ISO/IEC 27018 is the International Code of Practice for Personally Identifiably Information ('PII') Protection in Public Clouds Acting as PII Processors. The Office of the Privacy Commissioner of Canada – with input from representatives of the Government of Canada, other states and Data Protection Authorities – has significantly contributed to the development of the standard. It is not the only standard for data protection in the cloud, but it has unique value in that it:

- Offers a single, standardized, international set of privacy controls that align closely with existing privacy requirements;
- Integrates directly into a data security framework; and
- Has the highest compliance mechanisms through a certification process issued by an independent auditor and annual audits to ensure ongoing compliance.

This new standard holds certified cloud service providers to the following main obligations:

- Customer control: Store and use personal information exclusively in accordance with the instructions of the cloud customer and do not require the customer to consent to the use of their data for advertising and marketing purposes as a condition of their use of the service;
- Data retention: Establish a retention period after which customer data will be permanently returned or deleted;
- Accountability:
    - Disclose sub-processors of personal data, notify the cloud customer of any changes in sub-processors, and provide the customer the opportunity to terminate their agreement if they object to a change;
    - Promptly notify the cloud customer of any breach, unauthorized access to personal information or unauthorized access to processing equipment or facilities resulting in law, disclosure or alternation of personal information;
    - Disclose the countries in which a cloud customer's personal information might be stored; and
    - Undergo an annual audit by the cloud customer or by an independent auditor.
- Non-disclosure: Reject any requests for personal information disclosure that are not legally binding and consult with the relevant cloud customer unless notification is prohibited (for example, if it compromises an investigation); and
- Safeguards: Implement technical and organizational measures to safeguards to protect personal information

The main advantages of ISO/IEC 27018 for the MUSH sector are as follows:

- Selecting a cloud service provider that is ISO/IEC 27018 compliant supports the cloud customer's due diligence efforts;
- The annual independent audit required by ISO/IEC 27018 provides the cloud customer ongoing assurance that the cloud service provider remains in compliance with the standard's requirements; and
- Because ISO/IEC 27018 is built on ISO/IEC 27001 and 27002, the cloud service customer benefits from the enhanced security of a cloud service that adheres to international security standards.

Frequently asked questions

- Question: Are data centers in the United States subject to the USA PATRIOT Act?
    - Answer: Yes, and the sharing of data between Canadian and US law enforcement agencies occurs whether or not information is stored in the cloud. However, ISO/IEC 27018 requires cloud service providers to deny any request for personal information from law enforcement authorities without consent unless there is a legally binding authority, and even then the cloud provider will consult the cloud customer, unless prohibited by law. Customers should negotiate this requirement with their non-certified cloud provider.
- Question: Is the encryption up to the customer?
    - Answer: The customer may encrypt its own data. Certain cloud service providers may also encrypt the data 'in transit' between its customers and its service, between its data centres, and 'at rest'.
- Question: Can personal data be mined in the cloud for advertising/marketing purposes?
    - Answer: Yes, with the customer's consent. However, ISO/IEC 27018 prohibits a cloud service provider from making such consent a mandatory condition for using the service. The cloud provider holds the information on behalf of the customer much like a bank holds deposits in a safety deposit box on behalf of its customers.
- Question: How effective are contractual obligations to protect data?
    - Answer: A cloud provider that has made the significant investment to bring its operations in line with ISO/IEC 27018 to obtain certification, and whose business rests on that certification, will treat ISO/IEC 27018 obligations with the utmost seriousness. Breach of those obligations could result in the cloud provider failing an audit and losing its certification. If a cloud customer relies solely on contractual terms, it may not know if the cloud service provider is complying with those obligations absent a private audit (which the customer may not have the contractual right to demand, and if it does, may be too costly to be practical).
- Question: Which laws apply to cloud service providers?
    - Answer: In Canada, the cloud customer is responsible for ensuring that the cloud provider that receives the data for processing provides a "comparable level of protection [to which the cloud customer is obligated under Canadian law] while the information is being processed" by the cloud provider. This is ensured by contractual or other means.
- The cloud provider is bound by contract to respect the data protection obligations of the cloud customer. ISO27018 certified cloud providers also undertake to offer "support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed (between) the public cloud processor and its clients (cloud service customers)". However, the cloud provider is also bound by the law applicable in the territory where it is located. For that reason, requests from government authorities of the territory of the cloud provider apply to disclosure of that data. It is with that in mind that ISO 27018 requires certified cloud providers to disclose to the cloud customers the location of their servers as well as the countries of origin of their sub-contractors.

Five significant cloud service providers have achieved compliance with ISO/IEC 27018: Amazon, Dropbox, Google, IBM and Microsoft.

Chantal Bernier: Data breach response is 'not the time to improvise'

JULIUS MELNITZER | November 19, 2014 7:20 AM ET
More from Julius Melnitzer

"We're in a time warp, having jumped into a digital area that bring complexities in digital protection that we have not yet mastered completely," says Chantal Bernier

Photo: Don Healy / Postmedia News

***Chantal Bernier** is one of Canada's premier experts on privacy and security law. As former interim privacy commissioner and assistant privacy commissioner of Canada for over five years, she oversaw the operations of the Office of the Privacy Commissioner (OPC), including some of the country's highest-profile privacy investigations, privacy audits and privacy impact assessment reviews. She was also instrumental in defining new guidelines and regulations. Last month, she joined Dentons Canada LLP's privacy and security practice in Toronto as counsel. She spoke with **Julius Melnitzer**. This is an edited transcript.*

Q. Why is vulnerability to privacy and data breaches such a broad phenomenon in the business community?

A. We're facing relentless attacks that outpace the ability of organizations to protect themselves. There are a number of reasons for this: we're in a time warp, having jumped into a digital area that brings complexities in digital protection that we have not yet mastered completely; our amazement at the possibilities of new technologies sometimes blinds us to the privacy risks; and we trust experts to deal with information protection rather than fully integrating it. That's changing and CEOs are now engaging, but privacy protection and data security still need to become a central corporate issue at the same level as financial or human resource management.

Q. Can you provide some practical tips to safeguard businesses from cybersecurity breaches?

A. I would recommend using my Special Report following the loss of a hard drive at Employment Canada as a reference. Basically, there are four types of control, all independent of each other, that must be ensured: first, there are the old physical controls like

locks; second, technological controls like firewalls and encryption; third, administrative controls that produce proper policies; and fourth, personnel who are well-trained and supervised in their use of new technological platforms.

Q. What can companies do to minimize disruption and damage to the business and the brand if a breach does occur?

A. Most importantly, it's not the time to improvise. A breach response plan must be in place beforehand. When a breach occurs, the plan must be implemented immediately and the breach response escalated to the proper levels of management. Affected individuals must be notified so they can protect themselves and to demonstrate that the organization deserves trust. OPC should be notified right away if there is an obligation to do so, but even if there is no obligation it's a good idea to do so if the breach is serious — because it shows accountability. An organization should also offer credit monitoring to those affected, always have someone on call to communicate with affected persons and show proper support in other ways.

Q. What differentiates good companies from bad ones in terms of security safeguards and breach response?

A. Obviously, the fact that there's been a breach does not make a company a bad one. That's determined by examining the quality of the safeguards in place, the implementation of industry standards, the impact of the breach and the ease with which the breach occurred. The second test looks at the effectiveness and openness of the breach response, which is a test of the honesty and integrity of the organization.

Q. The Supreme Court of Canada recently ruled that personal information can't be disclosed without a warrant. What should the business community take away from that decision?

A. The *Spencer* case brought clarification to an issue that was outstanding during my entire time at OPC, which is whether basic subscriber or customer information was private information or public phone book information. The argument was made that it was merely phone book information, because if there was an Internet phone book, the information would be found there. My argument and privacy advocates' argument is that basic subscriber information (BSI) leads to very sensitive information because it's a clue to what is in a person's mind. It is highly revealing of interests, allegiances, concerns, health preoccupations, affiliations and other things. You notice that basic subscriber information is a very intimate space because there is a huge outcry from the public every time there is a proposal to increase investigative powers over the Internet. So what businesses need to take from *Spencer* is that private information can't be disclosed without a warrant or court order except in exigent circumstances, meaning immediate danger to personal safety.

Q. What are some of the limits on privacy rights?

A. One of the most significant is freedom of expression, which is in inherent juxtaposition to privacy rights and constantly arises as an issue. In another recent case involving the United Food and Commercial Workers, the SCC struck down Alberta's privacy law because it limited the right of unions to videotape persons who crossed the picket lines, which was seen as important to unions' right to freedom of expression. Businesses should be aware, then, that there may be contours around privacy rights when they come into conflict with other rights, particularly freedom of expression.

Financial Post

Five Golden Rules for Accountability on Privacy and Cybersecurity

Chantal Bernier, Counsel, Global Privacy and Cybersecurity Group, Dentons LLP Canada, former Interim Privacy Commissioner of Canada.

The vulnerability of information on digital platforms constitutes an unprecedented risk and the undermining of customer trust goes straight to the bottom line.

This calls for a new governance framework from top to bottom where,

- Board members hold senior management accountable for cyber-security and privacy as they do for financial integrity: without knowing all the right answers, but knowing all the right questions.
- CEOs are where the buck stops for cyber-security and privacy policies as for any issue integral to profitability, effective management, workplace ethics and consumer trust.
- CPOs and CIOs work together understanding their inherent overlap: if personal information resides in cyber-infrastructure, privacy resides in cyber-security.
- Business line managers ensure implementation of cyber-security and privacy policies through staff supervision and training.
- Staff endorse cyber-security strategies as a matter of ethics, honouring consumer trust.

Chantal Bernier, Counsel,
Dentons LLP Canada
+1 613 783-9684
chantal.bernier@dentons.com

ISO/IEC Standard 27018 provides a cloud breakthrough

The project had widespread support from national standards bodies. **Chantal Bernier** explains the benefits for companies.

ISO/IEC Standard 27018, Code of practice for PII protection in public clouds acting as PII processors, is a breakthrough. After years of dedicated work from Data Protection Authorities (DPAs), governments and industry representatives, on April 25 2014, the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) adopted Standard 27018 as a universal standard for certification of cloud providers' compliance with its privacy protection requirements.

Their efforts have borne fruit. Microsoft is the first cloud provider to receive certification on the basis of its incorporation of the controls and best practices of ISO/IEC27018 .

The importance of ISO/IEC 27018 rests upon two main considerations, in my view. First, it is evident from the exponential growth of cloud computing. The cloud computing industry has grown 300% from 2008 to 2014. This makes cloud computing growth rate 5 times higher than that of global IT.[3] In the same vein, the New South Wales Privacy Commissioner specifically recommends in her latest report to Parliament that "ISO/IEC 27018 standard covering privacy, security and cloud services be considered for inclusion in the NSW Government's Information Security Systems Policy."[4]

> The Standard enables cloud processors to be transparent.

This development should be celebrated for many reasons that relate to data protection However, it is also a milestone in the global harmonisation of privacy law and in the Data Protection Authorities' (DPA's) efforts in that regard. First, in the resolution of the International Conference of Data Protection Authorities in Montreal, in 2007, DPAs resolved to work more closely with ISO to contribute to the development of international data protection standards[1]. Second, in 2012, at the International Conference in Punta del Este, in a Resolution on Cloud Computing, DPAs called for, in particular:

- Privacy on the cloud
- Privacy impact assessments by organisations before moving to the cloud
- Transparency, accountability by cloud providers and contractual clauses that protect privacy
- Further efforts into research, third party certification and standardisation to achieve the desired level of trust and privacy on the cloud.[2]

Second, it is crucial to organisations that hold a high volume of sensitive data with limited resources for data security, such as schools, hospitals or small and medium business. These organisations will have their data much better protected in the cloud, with higher security, at lower cost. It is all the more critical for these resource-strapped organisations, such as schools, or small municipalities, that hold sensitive data without the means for appropriate safeguards. For example, 14% of cloud customers report having downsized their IT services after having adopted cloud services.[5]

That is why this new Standard for privacy on the cloud deserves such careful attention: the reduced cost and increased efficiency of the cloud make it the go to solution.

This article describes the main features of ISO/IEC 27018 and how it addresses long-standing privacy concerns about the cloud.

Background

ISO and IEC form the worldwide system for standardisation. They are composed of national bodies to develop international standards through technical committees.[6]

ISO/IEC Standard 27018 was developed by the ISO/IEC Joint Technical Committee with the following objectives:

1. Help public cloud providers comply with legal obligations when acting as personal data processors;
2. Enable data cloud processors to be transparent;
3. Assist cloud service customers and cloud providers to enter into contractual agreements;
4. Provide cloud customers with a mechanism to exercise audit and compliance rights on the cloud[7].

The benefits of cloud computing

The Office of the Privacy Commissioner of Canada (OPC) identifies the main benefits of cloud computing as:

1. Scalability, by offering unlimited storage and processing capacity;
2. Reliability, since it eliminates the risk of losing paper, laptops or hard drives and allows access to documents and applications via Internet worldwide;
3. Cost savings, since resources are pooled for optimal safeguards thus eliminating the need for investment in infrastructure;
4. Efficiency, as the freeing up of resources through the pooling of expertise allows focus on other priorities; and
5. Access to new technology as the cloud providers, being more

resourceful and specialised in the area, are in a position to offer a much wider choice[8].

The UK Information Commissioner's Office (ICO) states the advantages of the cloud as "increased security, reliability and resilience for a potentially lower cost."[9]

France's Commission Nationale de l'Informatique et des Libertés (CNIL) summarises the benefits of the cloud as the pooling of data storage and operational costs.[10]

Sensitivity about the cloud addressed with ISO/IEC 27018

The CNIL also summarises the "sensitive issues" ("questions délicates") about the cloud, namely, accountability; data transfers and jurisdiction; security; transparency; and qualification of the cloud provider.[11]

With a view to addressing these issues, ISO/IEC27018 was adopted.

1. Accountability

Perhaps the most important feature of ISO/IEC 27018, particularly for cloud customers that may not have the means to stand up to big cloud providers, is the provision for an audit of the cloud provider. The cloud provider must agree to audits either by the cloud customer or by an independent auditor. In addition, the Standard holds the cloud provider to:

- Designating a contact person regarding the implementation of the cloud computing contract
- Clearly describing in contractual agreements the allocation of responsibility between the cloud provider, its sub-contractors and the cloud service customer
- Promptly notifying the cloud customer of a data breach
- Establishing a mechanism to ensure internal compliance with privacy protection laws of the cloud customer
- Logging events and monitoring events logging with documented periods to apply necessary remediation.

In short, the compliance requirements are high and the compliance assurance measures are robust.

2. Data transfers and jurisdiction

Particularly since the Snowden revelations of June 2013, data transfers on the cloud raise concerns about data sovereignty and data control. ISO/IEC27018 squarely addresses the issue of data control and jurisdiction over data on the cloud with the obligation for the cloud provider to:

- Act only upon the instructions of the cloud customer and to operate the cloud in accordance with the privacy law applicable to the cloud customer, which excludes the possibility of data mining by the cloud provider, unless as directed by the cloud customer and in accordance with privacy law applicable to the cloud customer
- Disclose to the cloud customer the geo-location in which the personal data may be stored
- Reject any request for disclosure from law enforcement authorities that is not legally binding and consult the cloud customer before making any disclosure, unless prohibited to do so by law.

In fact, the cloud provider, under ISO/IEC 27018, commits to supporting and managing compliance with the privacy law applicable to the cloud customer.

3. Security

ISO/IEC 27018 augments security standards in the cloud by holding cloud providers to:

- Encrypt data transmitted over public data transmission networks
- Implement contracts with sub-contractors that specify security measures to protect data
- Notify promptly any data breach
- Implement human resource security measures, access controls, physical security, operations security, and information security incident management
- Retain data strictly within the bounds of the cloud computing contract. In addition, ISO/IEC 27018 specifies that cloud providers will commit to erasure of temporary files and disposal of the data within contractually set times with the data customer.

These provisions are in addition to the technological reality that, through pooling and dedicated expertise, a certified cloud will have far higher safeguards than most organisations' IT systems.

4. Transparency

As mentioned above, long-standing concerns are raised about the cloud relating to the opacity of undefined technical and administrative measures adopted by cloud providers to protect data.

Certification under ISO/IEC 27018 holds cloud providers to be transparent by:

- Providing cloud customers with information about their policies and practices
- Facilitating the exercise of individuals' right to access or correction of their personal information; and
- as mentioned above, disclosing the location of every server and the occurrence of any data breach.

5. Qualification of the cloud provider

The certification process under ISO/IEC 27018 addresses the final "sensitive issue" raised in the CNIL's guidance document: who is a qualified cloud provider?

ISO certification is issued by an accredited certification body after assessment of an organisation in relation to the Standard. When certification is issued, maintenance is subject to scheduled audits. Where auditors find compliance issues, corrective action is mandated or certification is revoked. Certification may also be revoked on the basis of an incident, outside an audit, that reveals non-compliance with the Standard.

Hence, there is now an authoritative way to find a qualified cloud: it is an ISO/IEC 27018 certified cloud.

ISO certification is issued by an accredited certification body upon assessment of an organisation in relation to the Standard.

Conclusion

Moving to the cloud represents the most secure and cost effective measure for data storage and reaching the highest guarantee for privacy compliance through ISO/IEC270128.

It seems to me there is little choice: organisations big or small, private or public, well-resourced or not, are moving to the cloud. It offers cloud customers lower costs, greater security and increased efficiencies for IT services.

Moving to the cloud is a business decision, which must be informed by privacy considerations. A collection of best practices from regulators and business point to these actions as key due diligence in adopting cloud computing:

1. Conduct a privacy impact assessment prior to adopting cloud computing.
2. Select an ISO/IEC27018 certified cloud provider or one that will commit to the same contractual obligations. Of course, in the latter case, there is no certification of privacy protection as there is under ISO/IEC27018 by an independent body.
3. If the cloud provider is not an ISO/IEC27018 certified cloud, verify the history of data security of the cloud provider.
4. Triage the data to be stored on the cloud according to sensitivity, to select whether to allow data to be stored in clear text, or encryption. That being said, ISO/IEC 27018 provides for encryption of data transmitted over public data transmission networks.
5. Assess existing IT infrastructure and organisational needs, to decide what data should be kept on internal servers and what should be stored in the cloud.

With that, we have the highest protection and highest accountability, at the lowest cost. Cloud 9.

AUTHOR

Chantal Bernier, LL.B., LL.M, Counsel, Global Privacy and Security Law Group, Dentons Canada LLP, former Interim Privacy Commissioner of Canada, Senior fellow, Graduate School of Public and International Affairs, University of Ottawa.

REFERENCES

1 Resolution on Development of International Standards, 29th International Data Protection and Privacy Authorities Conference, Montreal, 2007.
2 Resolution on Cloud Computing, 34th International Data Protection and Privacy Authorities Conference, Punta del Este/Canelones, 2012.
3 Syntax, February 10, 2014.
4 Report of the Privacy Commissioner under Section 81B of the Privacy and Personal Information Protection Act of 1998, February 2015, http://www.ipc.nsw.gov.au/sites/default/files/file_manager/20150212_Privacy%20_Commissioner%20Report_fINAL_low-res.pdf.
5 Siliconangle, January 27, 2014.
6 Code of practice for PII protection in public clouds acting as PII processors, ISO/IEC Standard 27018, p.vi.
7 Id page vii.
8 Report on 2010 OPC Consultations on Online Tracking, Profiling and Targeting and Cloud Computing, May 2010.
9 Guidance on the Use of Cloud Computing, ICO, 2012, https://ico.org.uk/for-the-public/online/cloud-computing/.
10 Cloud computing: les conseils de la CNIL pour les entreprises qui utilisent ces services, 2012.
11 id supra.

Main vulnerabilities and best practices in data protection: A view from the inside

Chantal Bernier, Counsel, Dentons LLP Canada, former Interim Privacy Commissioner of Canada.

Over five and half years at the Office of the Privacy Commissioner of Canada (OPC), I have read countless breach notifications from public and private organisations. Depending on the severity of the breach, assessed according to the gravity of consequences on individuals and the depth of failings of the organisation, some breaches were merely acknowledged, others were resolved and others were investigated. On the basis of this experience, I have observed three main vulnerabilities that cut across all types of organizations.

This article seeks to share insights as an "alert", so to speak, to the vulnerabilities to watch for in protection of personal information. It is also an observation on some best practices in that regard.

Vulnerability #1: cyber-security

This will come as no surprise. At best, it may be a confirmation that you are not alone. The sophistication and volume of cyber-attacks are pinning down even the most powerful, resourceful organisations. But in every case, no matter the size and status of the organisation, cyber-security breaches expose cyber-security vulnerabilities.

My remarks on this point relate to a composite of cases and the trends it shows. My experience and my discussions with managers bring me to alert organisations to two common mistakes in relation to cyber-security: underestimating risk and characterization of cyber-security as a strictly technological issue.

(a) Underestimating risks

Yes, it takes a thief to take a thief. Honest people do not assume dishonesty and malicious intent. A well-balanced CEO does not readily think that a young, lonely youth would find it amusing to disrupt a company's technological infrastructure. Also, too many business people, being more focussed on business than criminal trends, are unaware of the breadth of the underground economy of personal data theft and its high returns. The result is an insufficient focus and investment in cyber-security through underestimating risk.

Throughout the years and from my conversations with business people across the country I have drawn a few salient points on the phenomenon of underestimating risk:

Fascination with technology too often trumps vigilance about its risks. In a move to innovate, some organisations step away from the beaten path (for example, by adopting Bring Your Device – BYOD- policies) before mastering all the risks.

Technological protection of personal data is often seen as accessory, even extrinsic, to the company's line of business (renovations, kitchen appliances, textile, etc…) and, even in big businesses, senior management is not sufficiently seized of cyber-security issues.

Also in both small and big business, under-estimation of risk and insufficient engagement of senior management leads to financial decisions that neglect investment in cyber-security. Yet, losses incurred by companies that have been breached, demonstrate how allocation of resources to cyber security up front can avoid heavy costs down the road.

Because the need for initial investment is minimal and start up is simple, the online world gives access to entrepreneurs who are ill-prepared and focussed on their business objectives at the expense of managing cyber-security risks.

In all cases, a greater alert to criminal trends, more diligence in information security and better integration of information security to business management would have spared the organisation money and embarrassment.

The federal government is no exception to this lure of technology ahead of a complete assessment of risk. When I led the OPC 2010 Audit of Wireless Technology in Certain Federal Entities, we found that none of them had completed Threat and Risk Assessments (TRAs) before adopting the technology. It would not be unreasonable to extrapolate this finding to the private sector. At the very least, it may serve as a warning for us all on underestimation of risk.

(b) Approaching cyber security as strictly a technological issue

The OPC technologists have supported me in many complex files. They often took me to the conclusion that a technological breach was not necessarily a failing of the technological infrastructure but rather the failing to see cyber-security as a multi-faceted ecosystem. They taught me that cyber-security rests upon an ecosystem of protection grouping four main components: (*i*) physical controls (locks, access restrictions, access supervision…); (ii) technical controls (encryption, access controls, TRAs…); (iii) administrative controls (assets management, inventory, identification of assets…) and (iv) personnel security (suitability, training, supervision, disciplinary measures…). As in any eco-system, the components are inter-dependent, and when one fails, all fail. The OPC investigation I made public in 2014 on the loss at Employment and Social Development Canada (ESDC) of a hard drive containing the personal information of nearly 600,000 Canadians is a useful illustration of this point.

In short, the investigation brought out the following: personal data relating to student loans, including financial data, had been saved on a portable hard drive; the drive was not identified, was not encrypted and was stored in a drawer that was not locked; no one had been assigned responsibility for protection of the drive and employees were not aware of its content nor of its vulnerability; it was not tracked by asset control and no one could track it or, at least, no one did.

Yet, the investigation also brought out that ESDC had robust polices and governance structures for information security. In addition it had a strong technological infrastructure.

It was in the interdependence of the components of the ecosystem that protection failed: policies that required physical protection of material were developed but not followed and their implementation was not supervised; technological criteria were stated but their application was not monitored. Asset management was deficient and training of employees did not match their level of responsibility.

What struck me most about this investigation is that it was about one of the most sophisticated and privacy protective organisations. However, there was insufficient integration of cybersecurity to overall departmental management at every level. Integration would have led to greater vigilance in relation to training, supervision and implementation of ongoing controls essential to personal data protection.

In my view, this example serves as a lesson to us all. I directed the investigation to deliver a Report of Findings that could serve as a reference manual for any organisation holding personal data. It may therefore serve as a guide for any public or private organisation.

Vulnerability #2: Human error

The case of ESDC is also an illustration of this second vulnerability: in this case as in so many others, it is human error that brings down the data protection regime. Human error is in fact the most common cause of data breach. On the basis of the cases I have dealt with, human error stems from two main failings: insufficient digital literacy and lack of monitoring.

(a) Insufficient Digital Literacy

As the chain is only as strong as its weakest link, failure in employee digital literacy will bring down the most robust privacy framework. Numerous incidents that have been made public demonstrate the consequences of insufficient employee digital literacy: for example, one employee left on a colleague's desk, with no physical protection, an unencrypted USB key containing medical information of nearly 5,000 people; the employee thought it was more secure than sending the information via email – the key was never seen again; others , as the OPC found in its 2010 Audit of Wireless Technologies in Certain Federal Entities, protect their portable devices with weak passwords, such as 1,2,3,4.

In none of such cases I have dealt with do I recall signs of malice. On the contrary, we were faced with a contrite employee who was ignorant of the technology afforded as a work tool. The organisation's failing was that of entrusting employees with technological tools without ensuring they have the knowledge to use them.

(b) Lack of Monitoring

An audit and an investigation I led at the OPC in the private sector come to mind in relation to this point.
One OPC audit found that a company had a sound framework of privacy policies and practices but needed increased monitoring to ensure compliance. For example, storage policies were clear but were not followed. Wiping used computers for re-sale was subject to clear procedures. Yet, out of the 149 computers the OPC examined, 54 had been put ready for re-sale while still containing data of the previous owner.

This discrepancy between the policy framework and its application underscores the importance of monitoring. Since then, the company has complied with all the recommendations of the OPC.

The investigation that is relevant here is one which revealed how an employee had issued a product without going through the company's privacy controls. And no one checked.

While the unlawful collection of personal information was inadvertent, it remains a failing of governance and monitoring within the company. It clearly did not have the governance framework to ensure compliance with privacy law nor the effective monitoring practice to verify it. This company as well accepted the recommendations of the OPC.

Vulnerability #3: Employee Snooping

The case of *Jones v. Tsige* (ONCA 2012), is only one among many. A bank employee was found liable for damages after violating privacy. She had accessed a person's financial information, over 100 times, for personal reasons.

Main vulnerabilities and best practices in data protection: A view from the inside

Privacy authorities across the country receive numerous complaints about unauthorised access by employees to their organisation's databanks. Main trends are around sentimental and financial issues. By way of example, employees access their organisation's data banks to seek financial information on their former spouses or on their former spouses' new partners; in one case, the employee had accessed the medical records of a former partner; another had unlawfully accessed the tax information of nearly two hundred persons directly or indirectly related to a new lover; others have sought and disclosed their organisation's information on celebrities.

Examples abound across the country and across types of organisation. The challenge, of course, is to ensure a system of access controls wide enough to allow efficient operations but restricted enough to avoid abuse.

It appears that the proper balance between an operational access control regime and privacy protection has not yet been achieved, even in well-resourced organisations. In Canada, repeated cases of such intrusions can lead to a determination of reasonable grounds to believe there is contravention of privacy law. This can be the basis of an OPC audit. Hopefully, this will serve as a call to action for organisations, all weakened by this vulnerability.

Best Practices

If the number of incidents, investigations and audits I have led has given me a basis to identify vulnerabilities, it has also provided me with an indication of best practices. They stem from the vulnerabilities I have described:

(a) Have an expert do a TRA before adopting new technology, and present it to senior management.

(b) Integrate data protection issues to management issues in general and to the management table.

(c) Submit the use of technology to adequate related training and ensure maintenance of that knowledge.

(d) To detect and avoid non-unauthorised access to your organisation's personal databanks, establish an audit trail system to track electronic access and a system for immediate notification of non-authorised access; also, subject physical access to appropriate restrictions according to the sensitivity of the data.

(e) Make employees responsible for protection of the data they control and ensure their proper supervision by their superiors in an efficient governance framework for compliance assurance throughout the organisation.

Finally, I refer you to a guide I developed with the Alberta and British Columbia Information and Privacy Commissioners entitled "Getting Accountability Right with a Privacy Management Program". The guide will provide you, I hope, with a methodical and verifiable approach to counter current vulnerabilities in data protection.

Chantal Bernier, Counsel
Dentons LLP Canada
+1 613 783-9684
chantal.bernier@dentons.com

A map of data residency requirements

大成 DENTONS

Country	Applicable Privacy Law	Specific Data Residency Requirements for Cloud Computing	Cross-Border Data Flow Regulations
Australia	• *The Australian National Privacy Act* (1988) • *Privacy Amendment (Enhancing Privacy Protection) Act* (2012)	No	Yes[i]
Canada	• *Privacy Act* (1993) – Federal public sector • *Personal Information Protection and Electronic Documents Act* [PIPEDA] (2000) – Federally regulated private sector • British Columbia, Alberta, and Quebec have provincial private sector laws. All other provincial private sector business is governed by PIPEDA. • Each province has a unique public sector statute.	*No, except, public bodies in British Columbia and Nova Scotia have an obligation to store data within Canada, except with consent.*	• *PIPEDA – No*[ii] • *Alberta – cross-border transfer requires notice* • *Quebec – requires assurance of equivalent safeguards*
China	• *Cybersecurity Law*[iii]	Yes	No
Colombia	• *Ley 1581 ("General Provisions for the Protection of Personal Data")* (2012) • *Decreto 1377 de 2013 ("Decree 1377")*	No	Yes
Europe	• *Directive on Data Protection* (1995) • The new *General Data Protection Regulation* will take effect in May 2018.	Yes	Yes
India	• *Information Technology Act* (2002) • Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Information) Rules 2011	No	Yes[iv]
Israel	• *Protection of Privacy Law, 5741-1981* • *Privacy Protection Regulations (Transfer of Data to Databases Abroad), 57612001*	No[v]	Yes
Mexico	• *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* ("Federal Law on the Protection of Personal Data Possessed by Private Persons") (2010)	No	Yes[vi]

A map of data residency requirements

Country	Applicable Privacy Law	Specific Data Residency Requirements for Cloud Computing	Cross-Border Data Flow Regulations
Russia	• *Federal Law No. 152-FZ* ("On Personal Data") (2006) • *Federal Law No. 242-FZ* ("On Introducing Amendments to Certain Legislative Acts of the Russian Federation with Regard to Personal Data Processing in Information and Telecommunications Networks") (2014) • *Federal Law 526-FZ* (amendments took effect September 1, 2015)	Yes[vii]	No[viii]
South Africa	• *Protection of Personal Information Act* (2013)	No	Yes[ix]
Switzerland	• *Federal Act on Data Protection* (1992)[x] • Additionally, each canton has a cantonal data protection act.	No	Yes
United States	• State-specific. However, the Federal Trade Commission has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations in specific areas (e.g. for telemarketing, spamming, and children's privacy).[xi] Additional regulations exist for employee information, health records, and financial details.	No	No

i Australian Privacy Principle 8 governs cross-border disclosure of personal information. It requires that the data controller take reasonable steps to ensure that the recipient does not breach the Australian Privacy Principles. Additionally, the Australian entity that discloses personal information to an overseas recipient is responsible for any acts or priactices that of the overseas recipient in relation to the information. See: Office of the Australian Information Commissioner: https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/chapter-8-app-guidelines-v1.1.pdf .

[ii] The *Personal Information Protection and Electronic Documents Act* (PIPEDA) does not prevent an organization from transferring personal information to an organization in another jurisdiction for processing. However, PIPEDA establishes rules governing those transfers—particularly with respect to obtaining consent for the collection, use and disclosure of personal information, securing the data, and ensuring accountability for the information and transparency in terms of practices. 'Fact Sheet: Cloud Computing', Office of the Privacy Commissioner of Canada, online: www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_02_e.asp.

[iii] Unofficial Translation of 2016 Cybersecurity Law: http://chinalawtranslate.com/cybersecuritylaw/?lang=en .

[iv] India has no registration requirements for any parties under the *Information Technology Act* 2001. However, there are some rules in place for the transfer of sensitive data offshore. It can only be transferred to a country where it is clear that the sensitive data will be adequately protected as per the Rules. 'Sensitive data' is defined under the 2011 Rules as information relating to a data subject's: password; financial information; health, sexual orientation; medical records and biometric information.

[v] No residency requirement for cloud computing, but any database which contains more than 10,000 data subjects, sensitive information, information collected without consent, database of a public entity, or database used for direct-marketing services must be registered with the Israeli Law, Information and Technology Authority (ILITA).

[vi] For cross-border data transfers, Mexican law requires notice to and consent from the data subjects, and makes the data controller responsible for ensuring that the recipient of the data abides by the same principles as those that are set forth in the sender's privacy policy.

[vii] Personal data on Russian citizens must be stored in databases physically located in Russia.

[viii] Data may be transferred out of Russia if it is first "recorded, systematized, accumulated, stored, amended, updated and retrieved" in a Russian database.

[ix] *Protection of Personal Information Act*, Section 72. This section is not yet in force. The *Protection of Personal Information Act* will limit cross-border transfers of personal information unless the recipient is subject to laws, binding corporate rules or contracts that establish the same level of data protection as the *Protection of Personal Information Bill*.

[x] *Federal Act on Data Protection*, amended as of 1 January 2014: https://www.admin.ch/opc/en/classified-compilation/19920153/201401010000/235.1.pdf

[xi] DLA Piper 'Data Protection Laws of the World March 2013', accessed 11 November 2016, at 492, online: https://files.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf.

Current as of November 23, 2016.

Chantal Bernier, Counsel
Dentons LLP Canada
+1 613 783-9684
chantal.bernier@dentons.com

The protection of Personal data in a New Context of Risk – Step by Step

Chantal Bernier, Counsel, Dentons LLP Canada, former Interim Privacy Commissioner of Canada.

1. Fundamentals

- A risk assessment geared to the organization's mandate, the sensitivity of the data and the ambient risks.
- A clear, customized and exhaustive set of policies.
- A specific and entrenched governance structure.

2. Implementation

(a) A set of policies,

- Based on an ecosystem of physical, technological, administrative and staff security controls,
- Published conspicuously and easily accessible,
- Comprising an early response protocol in the event of a breach.

(b) A governance structure to assure the implementation of and compliance with the practices, including,

- Data protection responsibilities shared internally,
- Institution of sufficient and effective remedies for users,
- Engagement at every level of the organization,
  - The Board must ensure accountability for protection
  - The CEO must assume organizational responsibility
  - The Privacy and IT officers must work in concert
  - The managers must oversee the practices
  - The employees must endorse and comply with the policies

3. Incident response

(a) Breaches

- Mobilization of the early response protocol,

- Determination of notification based on the real risk of serious harm,
- Strategic communication to the public and/or the affected individuals,
- Internal crisis management.

(b) Complaints

- Assistance to the complainant,
- Cooperation with the regulator,

A few points of reference:

OPC Investigation into the loss of a hard drive at Employment and Social Development Canada, March 25, 2014

Ten Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency, OPC, October 2013

Getting Accountability Right with a Privacy Management Program, OPC, 2012

ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Boards' Oversight for Privacy – It is About Knowing the Right Questions, Board Intelligence, Federated Press, http://www.federatedpress.com/boardroom-intelligence.html

Tab 5

Endgame: Limitation of Liabilities

Courageous Counsel Leadership Institute 2016

STAFFORD MATTHEWS
Managing Partner, Silicon Valley
T +1 650 798 0380
M +1 415 815 9850
stafford.matthews@dentons.com
dentons.com

SUSAN PONCHER GREENSPON
Partner, Chicago
T +1 312 876 3482
M +1 847 814 4999
susan.greenspon@dentons.com

COURAGEOUS COUNSEL

General principles

- **Limitation of liability** clauses in a contract by definition **narrow** the scope or **limit** the amount of damages or other liabilities to be borne by a party in the case of certain transactions or events. In general fully enforceable.
- Contrast with **exculpatory** clauses which seek to entirely exonerate a party from any liability for future conduct. Exculpatory clauses are disfavored and strictly construed under most state laws.* Matter of degree.

**See* Cal. Civ. Code § 1668; *Sommer v. Federal Signal Corp.*, 79 N.Y.2d 540, 554 (1992); *Empire Lumber Co., v. Thermal-Dynamic Towers*, 971 P.2d 1119 (Idaho 1998); *Scott & Fetzer Co. v. Montgomery Ward & Co.,* 112 Ill. 2d 378, 493 N.E.2d 1022 (Ill. 1986).

General principles

- The limitation of liability clause is the **endgame** of every contract negotiation. It is the last clear chance to manage ultimate risk in a transaction. A comprehensive limitation of liability clause can render many of the obligations under a contract **moot** as a practical matter.

- **Example - Ultimate Limitation**:

"IN NO EVENT SHALL THE TOTAL LIABILITY OF ALPHA CORPORATION ARISING OUT OF OR RELATING TO OR IN CONNECTION WITH THIS AGREEMENT OR THE SUBJECT MATTER HEREOF EXCEED FIVE MILLION DOLLARS (US $5,000,000) IN THE AGGREGATE."

Types of Limitations

(1) Limitation or exclusion from liability based on <u>classes</u> or <u>categories</u> of damages:

- A limitation clause usually will provide that damages are excluded or limited for certain **types** or **classes** of losses, for example, consequential or incidental or punitive damages.

Types of Limitations

(2) Limitation or exclusion based on the cause of the damages:

- A limitation of liability clause normally will provide that certain acts or omissions are **not limited** by the clause or are subject to higher limitation caps ("**carve-outs**"). Common examples are breach of confidentiality and fraud.
- Losses caused by other forms of breach or conduct would be subject to caps or entirely excluded as a class from liability.

Types of Limitations

(3) Limitation on the amount of damages:

- A limitation clause can provide that damages are capped and only recoverable up to a certain limit. This can be an attempt to pre-estimate the losses which might be incurred as a result of certain types of breaches or merely a blunt instrument to cap exposure by one or both parties.
- This can include various sub-classes or tiers of caps based on the specific cause of the breach or liability.

Types of Limitations

(4) Combination of Limitations:

A limitation of liabilities clause is usually comprised of at least two parts: (A) an outright **exclusion** from liability of certain classes of damages such as consequential damages, and (B) a broader **limitation of liabilities** as to all damages, such as by use of caps on the total amount of liability, other than exceptions that are expressly carved out of the clause and therefore will be unlimited.

Limitation of Classes

LIMITATION OF CLASSES OF DAMAGES

Limitation of Classes - Example

"Notwithstanding any contrary provision hereof or the failure of essential purpose of any limited remedy, to the fullest extent not prohibited by applicable law, neither party shall be liable for any **indirect, incidental, special, consequential, exemplary or punitive damages or losses** incurred by the other party or any [affiliate][other third person or entity] arising from or relating to this agreement or the subject matter hereof, **whether in contract, tort (including negligence), products or strict liability or any other form of action**, even if such party has been advised of the possibility of such damages or losses or such damages or losses were reasonably foreseeable."*

*Issues of conspicuousness of the clause are separately discussed below.

Classes: Direct versus Consequential Damages

Hadley v. Baxendale, (1854) 9 Ex. 341:

- Both **direct** damages and **consequential** damages are fully recoverable by a party under ordinary rules of damages.
- Other losses are not recoverable as being too **remote or speculative**.*

* *E.g., United States ex rel. Mms Constr. & Paving v. Western Surety Co.*, 754 F.3d 1194 (10th Cir. 2014).

Classes: Direct versus Consequential Damages

(1) Direct Damages: Damages flowing from the natural and probable consequences of the breach of the contract itself as between the parties themselves; the benefit of the contractual bargain of the plaintiff; "the direct and immediate fruits of the contract" * Also referred to as "**general**" damages.

Examples: Failure to pay for contracted for goods or services; failure to report and pay royalties; compensation for the value of promised performance.

**E.g., American List Corp. v U.S. News & World Report,* 75 N.Y.2d 38, 43, 550 N.Y.S.2d 590 (1989).

Classes: Direct versus Consequential Damages

(2) Consequential Damages: Losses that do not flow directly and immediately from a breach of the **type** of contract entered into between the parties − but are secondary damages which result from the effect of the breach on **other agreements** or **circumstances** of the **specific** parties. Also referred to as "**special**" or "**indirect**" damages.*

- Consequential damages "are one step removed from the naked performance promised by the defendant". *Schonfeld v. Hilliard*, 218 F.3d 164, 177 (2d Cir. 2000).

*These terms are imprecise and somewhat duplicative but the practice is to list all of them in this type of clause. Any express exceptions to a consequential damages exclusion should also reference indirect and special damages to be comprehensive and limit ambiguity.

Classes: Direct versus Consequential Damages

Consequential Damages:

- Includes claims arising from separate agreements or relationships between the plaintiff and **third parties** which are a **consequence** of the primary breach.
- Must be **reasonably foreseeable** by the breaching party at the time the contract was made.
- "Consequential damages" does **not** mean remote or speculative or unforeseeable damages, which the law does not permit.*

**See Darrow v. Phillips*, 2015 IL App (2d) 140763-U, P20 (Ill. App. Ct. 2d Dist. 2015)(severe emotional or mental disturbance from contract breach not foreseeable).

Classes: Direct versus Consequential Damages

Examples: customer or other third party claims for defective goods; loss of goodwill; loss of customers; harm to reputation; loss of market share; loss in value of business.*

Case Study: Grant of exclusive territory by Pepsi for bottling and sale of products; failure by Pepsi to prevent a competitor from selling into the territory; lost sales to customers held to be excluded consequential and not direct damages. *Compania Embotelladora Del Pacifico, S.A. v Pepsi Cola Co*., 650 F. Supp. 2d 314 (S.D.N.Y. 2009).

**Trimed, Inc. v. Sherwood Medical Co.*, 977 F.2d 885 (4th Cir. 1992); *RIJ Pharm. Corp. v. Ivax Pharms., Inc.*, 322 F.Supp. 2d 406 (S.D.N.Y. 2004).

Classes: Direct versus Consequential Damages

- Note that Section 2-715(2) of the **Uniform Commercial Code (UCC)** defines "consequential damages" from the seller's breach of a contract for the sale of goods as:

  "(a) any loss resulting from general or particular requirements and needs of which the seller at the time of contracting had reason to know…; and

  "(b) injury to person or property proximately resulting from any breach of warranty."*

*Caution: Under the Uniform Commercial Code, the buyer of goods is automatically entitled to consequential damages as a matter of statute but the seller is not, unless such consequential damages are expressly excluded by the contract. UCC § § 2-706(1), 2-708(1), 2-713(1), 2-715.

CORE POINT 1

- This is not an argument about whether or not the defendant has breached the contract or whether that breach has proximately caused the damages incurred by the plaintiff.
- It assumes that there **have been** material damages caused by the defendant. The core question is whether the defendant is being **excused or limited contractually from responsibility** for those damages it in fact caused.
- The limitation of liabilities clause **overrides** the entire rest of the contract, including indemnification provisions, depending on how it is constructed.

Classes: Consequential Damages Exclusion

(3) Consequential Damages Exclusion:

"NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL….DAMAGES OR LOSSES"

Classes: Consequential Damages Exclusion

- Standard in US commercial contracts. Generally enforceable under US law.*
- Limitation or exclusion of consequential damages **permitted** under Section 2-719(3) of the Uniform Commercial Code unless "**unconscionable**". Limitation of **commercial losses** generally is not considered unconscionable.**

**E.g., Logan Equip. Corp. v. Simon Aerials, Inc.*, 736 F. Supp. 1188, 1195 (D. Mass. 1990) ("Limitations on recovery of consequential damages in a corporate context represent 'a reasonable accommodation between two commercially sophisticated parties' which does not offend any public policy of the state'"); *Lindemann v. Eli Lilly & Co.*, 816 F.2d 199 (5th Cir. 1987).

**UCC § 2-719(3). *See Salt River Project v. Westinghouse Electric Corp*., 694 P.2d 198, 205 (Ariz. 1984)(unconscionability in contracts between commercial enterprises rare). See note on "unconscionability" below.

Classes: Consequential Damages Exclusion

- Basic rationale for **consequential damages exclusion** is that it represents an allocation between the parties of unknown or undeterminable risks, especially where the exclusion is mutual to both parties.*
- **But is this always justified?** By definition the parties must know or have reason to know of the potential for the **consequential** losses in the event of a breach. For example: where nonperformance by the defendant will cause the breach by the plaintiff of its downstream contracts with customers.

*Comment to UCC § 2-719(3).

Classes: Consequential Damages Exclusion

In each case consider:

- Whether consequential damages should be excluded. Most consequential damages in fact will always be caused by **only one of the parties:** usually the manufacturer or seller in the case of goods or the service provider. The concept of **mutuality** of these clauses is generally **false**.
- Generally in the interest of the **seller** to **exclude** all consequential damages and for the **buyer** to **minimize** the exclusion and preserve the right to sue for consequential damages that will result from a breach.

CORE POINT 2

- **Consequential damages** can be much broader in scope than direct damages.
- Consequential damages can represent the **core liability or loss** suffered by the plaintiff and can **substantially exceed** any direct damages.
- Must determine whether and how much to limit consequential damages in each case. Do not accept as **"standard boilerplate"** the consequential damages exclusion in the contract but deliberately assess the potential for loss in the event of a breach.

Classes: Exclusion of Lost Profits

Special Case: Exclusion for Loss of Profits

- Common misconception that **loss of profits** or other economic losses are always "consequential damages" and therefore limited by the consequential damages exclusion clause without more.
- Loss of profits in fact may be either **direct damages** or **consequential damages** depending on the case.*

**E.g., Coniber v Center Point Transfer Sta., Inc.*, 137 A.D.3d 1604, 1605-1606 (N.Y. App. Div. 4th Dep't 2016) (direct and not consequential damages when plaintiff "seeks only to recover money that the breaching party agreed to pay under the contract"; in that case the difference between the payments specified in the contract and the cost of plaintiff's performance of that contract); *Midland Hotel Corp. v. Reuben H. Donnelley Corp.*, 118 Ill.2d 306, 515 N.E.2d 61 (Ill. 1987)(profits held to be the "basis of the contract" and thus direct damages); *Oliver B. Cannon & Son, Inc. v. Dorr-Oliver, Inc.*, 394 A.2d 1160, 1163 (Del. 1978).

Classes: Exclusion of Lost Profits

Biotronik AG v Conor Medsystems Ireland Ltd., 22 N.Y.3d 799, 988 N.Y.S.2d 527 (N.Y. 2014):

- Distributor (Biotronik) purchased medical stents from manufacturer (Conor) for a purchase price based on a percentage of Biotronik's net sales. Conor withdrew stents from the market and Biotronik sued for $100 Million in lost profits from projected resales over the term of the contract.
- Standard consequential damages exclusion in the contract had no reference to "loss of profits". Conor claimed these were consequential damages and should be excluded.

Classes: Exclusion of Lost Profits

- New York Court of Appeals in Biotronik held that the lost profits were **direct damages** and not barred by the consequential damages exclusion.
- The court reasoned that the purchase price to the manufacturer under the contract was **dependent upon** and computed under a formula based on resales by the distributor and therefore was considered more similar to a "joint venture".
- The loss of profits from resales therefore was considered to flow directly from the contract itself.

Classes: Exclusion of Lost Profits

- The Biotronik court held that while losses from a separate agreement with a third party are generally consequential damages, this "does not mean that lost resale profits can never be general damages simply because they involve a third party transaction" and that this determination must be made on a case by case basis.
- The Biotronik decision has implications for any contract where the consideration between the contract parties is dependent upon or connected to third party transactions outside of the contract. This includes **intellectual property licenses** and **other royalty or revenue sharing based** contracts.

Classes: Exclusion of Lost Profits

Takeaways from Biotronik:

- Must intentionally determine whether to **exclude or not exclude** lost profits or similar losses (such as lost revenues or loss of opportunity) as damages. May be the main damages suffered by a party in a failed deal.
- The consequential damages exclusion must be very carefully drafted to implement this determination. If intended the clause should clearly state that it covers both direct and consequential loss of profits.

Classes: Exclusion of Lost Profits - Other Issues

- **Types of Contracts:** Certain other types of contracts are susceptible to claims that lost profits are **direct damages** in addition to the Biotronik type of situation.
- **Example:** Some courts have held that lost profits are direct damages in **non-competition or trade secret** agreements where protection against lost profits is the precise benefit being bargained for.*

**E.g., eCOMMERCE Indus. v. MWA Intelligence, Inc.*, 2013 Del. Ch. LEXIS 245 (Del. Ch. Sept. 30, 2013).

Classes: Exclusion of Lost Profits - Other Issues

- **Illusory Contracts:** An exclusion of **both** direct and consequential "lost profits" damages also could render the contract **unenforceable and illusory** if lost profits is the only available measure of direct damages.*
- Consider whether it is appropriate to exclude direct lost profits under the circumstances.

**See, e.g., Tractebel Energy Mktg. v. AEP Power Mktg.*, 487 F.3d 89, 109-110 (2d Cir. 2007); *M&G Polymers USA, LLC v. Carestream Health, Inc.*, 2010 Del. Super. LEXIS 161 (Del. Super. Ct. Apr. 21, 2010). See the general discussion below on illusory agreements.

Classes: Lost Profits - Text Example 1

Compare:

"NEITHER PARTY SHALL BE LIABLE FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, **INCLUDING DAMAGES FOR LOST PROFITS**"

- There is a split in the cases: Some courts hold that this type of language **does not exclude** lost profits if in fact direct damages and only excludes lost profits to the extent such losses constitute consequential damages.*

*Compare, e.g., *Penncro Assocs., Inc. v Sprint Spectrum, L.P.,* 499 F.3d 1151 (10th Cir. 2007) and *Gardensensor, Inc. v. Stanley Black & Decker, Inc.,* 2014 U.S. Dist. LEXIS 135302, 5-6 (N.D. Cal. Sept. 24, 2014) (does not exclude direct damages) *with Quicksilver Res., Inc. v Eagle Drilling, L.L.C.,* 2009 U.S. Dist. LEXIS 39176 (S.D. Tex. May 8, 2009)(excludes).

Classes: Lost Profits - Text Example 2

Compare:

"NEITHER PARTY SHALL BE LIABLE FOR ANY **LOST PROFITS** OR ANY **OTHER** SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES"

- Same problem: Ambiguous as to whether direct damages in the form of loss of profits are excluded under the clause, or are only a subset of consequential damages.

Classes: Lost Profits - Text Example 3

Compare:

"NEITHER PARTY SHALL BE LIABLE FOR [**ANY LOST PROFITS** OR] ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL [OR **LOST PROFITS]** DAMAGES"

"NEITHER PARTY SHALL BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SIMILAR DAMAGES, **LOST PROFITS**,…."

- Excludes from liability **both** direct and consequential damages for lost profits.*

**Vaulting & Cash Servs. Inc. v. Diebold*, 1999 U.S. App. LEXIS 39386,199 F.3d 440 (5th Cir. 1999); *Imagine Sys. International v. Magnetic Resonance Plus, Inc.,* 227 Ga. App. 641 (1997).

Classes: Lost Profits - Text Example 4

Compare - More Targeted Clause:

"NEITHER PARTY SHALL BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR LOST PROFITS DAMAGES OF ANY KIND, **OTHER THAN** LOST PROFITS OR OTHER DAMAGES BASED ON THE CLAIMS OF AN UNAFFILIATED THIRD PARTY TO THE EXTENT (i) PROXIMATELY CAUSED BY THE BREACH OF THIS AGREEMENT AND (ii) AWARDED IN A FINAL AND NONAPPEALABLE JUDGMENT OR ARBITRATION AWARD AGAINST THE NON-BREACHING PARTY IN ACTIONS OR PROCEEDINGS ON SUCH THIRD PARTY CLAIMS."

CORE POINT 3

- Exclusion of **"lost profits"** from liability requires conscious analysis of the circumstances of your transaction.
- If your company is the probable plaintiff: **carve out "**lost profits" from the consequential damages exclusion, or at a minimum expressly provide that any "lost profits" exclusion applies **only to consequential damages** and not to any **direct damages** incurred by the company.
- If your company is the probable defendant, draft the exclusion clause to maximize the scope of the exclusion and avoid the foregoing mistakes in drafting. Consider whether a total ban on "lost profits" damages could invalidate the contract as illusory if no other remedies.

Classes: Exclusion of Hybrid Losses

- **Distinguish "Hybrid Damages":**
  - Damages for the loss of an income-producing asset are sometimes referred to a "hydrid" damages. Hybrid damages are usually consequential damages but considered a **separate and distinct class** of damages from lost profits.*
  - Hybrid damages generally based on **the fair market value** of the asset - considered the value of the "chance" to earn profits - as opposed to the lost profits themselves.**

**Schonfeld v. Hillard*, 218 F.3d 164, 176 (2d Cir. 2000); *Packgen v. Berry Plastics Corp.*, 46 F. Supp. 3d 92, 112 (D. Me. 2014).

*** Spectrum Sciences & Software, Inc. v. United States*, 98 Fed. Cl. 8, 16 (Fed. Cl. 2011).

Classes: Exclusion of Hybrid Losses

- Therefore, contractual exclusion of "lost profits" from liability per se **may not be sufficient** to bar **hybrid damages** based on the loss of an income-producing asset.
- Note that the breach of a contract to deliver or enter into a separate supply or license agreement or other contract providing for payments to the plaintiff may constitute both (1) **direct damages** rather than consequential damages and (2) **hybrid damages** not covered by a "lost profits" exclusion, in the same manner as the failure of the defendant to deliver any other contracted for asset.*

* *See Schonfeld v. Hillard*, 218 F.3d 164, 176-77 (2d Cir. 2000)(supply agreements as a form of intangible property with an ascertainable value)

Classes: Other Consequential Damages

- Diminution in value
- Business interruption or delay
- Loss of opportunity
- Loss of goodwill
- Loss of market share
- Loss of use
- Loss of data
- Breach of data protection or privacy laws for third party personal information
- Value of internal time of company employees

Classes: Exclusion of Torts or Punitive Damages

- The limitation of liability clause can be expanded to include the exclusion or limitation of **noncontractual claims** - including **torts** or **strict liability** - as between the parties.*
- However exclusions for breach of **statutory obligations** can be unenforceable in certain jurisdictions.**

* *Benchmark Elecs., Inc. v. J.M. Huber Corp*., 343 F.3d 719, 726–28 (5th Cir. 2003); *Kuehn v. Childrens Hosp*., 119 F.3d 1296, 1302 (7th Cir. 1997); *Food Safety Net Services v. Eco Safe Systems USA, Inc*., 209 Cal. App. 4th 1118; 147 Cal. Rptr. 3d 634 (Cal. App. 2012).

** Cal. Civ. Code § 1668 (discussed below).

Classes: Exclusion of Torts or Punitive Damages

- **Negligence:** Liability for ordinary negligence generally can be excluded by:

  (1) Use of the words "negligent" or "negligent acts"

  (2) Use of terms such as "tort" and "strict liability" or "products liability" or overall financial caps in the case of sophisticated parties.*

**McDermott, Inc v. Iron*, 979 F.2d 1068 (5th Cir. 1992); *Lincoln Pulp & Paper Co. v. Dravo Corp., 436* F. Supp. 262 (E.D. Pa. 1977).

Classes: Unenforceable Exclusions from Liability

- Certain exclusions or limitations - including the consequential damages exclusion clause - will **not** be enforceable if the terms violate **public policy** or are **unconscionable**.**

* *Benchmark Elecs., Inc. v. J.M. Huber Corp*., 343 F.3d 719, 726–28 (5th Cir. 2003); *Kuehn v. Childrens Hosp*., 119 F.3d 1296, 1302 (7th Cir. 1997); *Food Safety Net Services v. Eco Safe Systems USA, Inc*., 209 Cal. App. 4th 1118; 147 Cal. Rptr. 3d 634 (Cal. App. 2012).

** See note on "unconscionability" below.

Classes: Unenforceable Exclusions from Liability

- **Gross Negligence:** Unenforceable in most jurisdictions on public policy grounds.*
- **Willful misconduct, malice or intentional wrongdoing:** Unenforceable in most jurisdictions on public policy grounds.

  Note that New York law uses an "intent to harm" standard: an intentional breach of contract out of legitimate economic self-interest and not with an intent to inflict economic harm on the plaintiff is not against public policy and can be subject to a limitation of liability.**

Kalisch-Jarcho, Inc. v. New York, 448 N.E.2d 413, 416 (N.Y. 1983); *City of Santa Barbara v. Superior Court*, 41 Cal. 4th 747, 62 Cal. Rptr. 3d 527 (2007).

** *Kalisch-Jarcho, Inc. v. New York, supra* (reckless disregard; intent to harm)*; Metropolitan Life Ins. Co. v Noble Lowndes International, Inc*., 84 N.Y.2d 430 (N.Y. 1994);

Classes: Unenforceable Exclusions from Liability

- Note however that in many US jurisdictions (including New York) the term "**willful**" is not defined, especially if used alone without any reference to misconduct [such as "any willful acts"] . In those cases the exclusion from the limitation of liability can face issues of scope.*
- **Best practice** is for the parties to define "willful" in the clause. For example: "For purposes hereof 'willful' shall mean fraudulent, malicious or based on a sinister intention to harm or act in bad faith"; or "For these purposes 'willful' means an intentionally malicious or tortious act."

Metropolitan Live Insurance v. Noble Lowndes International*, 84 N.Y.2d 430 (1994); *Banc of America Securities v. Solow Building Co*. 47 A.D.3d 239, 244 (2007). Note that use of terms such as "intentional" or "willful" standing alone can make the exclusion **much too broad, thus depriving a party of the expected protection of the limitation of liability. Most acts of a party in a transaction are intentional but not malicious or with intent to harm.

Classes: Unenforceable Exclusions from Liability

- **Fraud and Fraudulent Misrepresentation:** Exclusion from liability for fraud or fraudulent misrepresentation unenforceable in most jurisdictions, although different states apply varying standards.*
- In the case of **fraud in the inducement**, the contract itself is voidable under most state laws and therefore the limitation of liability clause generally would not be enforceable in the case of a rescission.**

*Cal. Civil Code § 1668; *Kleinwort Benson N. Am., Inc. v. Quantum Fin. Servs., Inc*., 285 Ill.App.3d 201, 216, 220 Ill.Dec. 457, 467, 673 N.E.2d 369, 379 (1st Dist.1996); *Zircon Co. v. Graphik Dimensions, Inc.*, 1996 Mass. Super. LEXIS 227 (1996).

***See Pfizer Inc. v. Stryker Corporation*, 348 F. Supp. 2d 131 (S.D.N.Y. 2004); *Airborne Health, Inc. v. Squid Soap, LP*, 984 A.2d 126 (Del. 2009); *ABRY Partners V, L.P. v. F & W Acquisition LLC*, 891 A.2d 1032, 1061 (Del. 2006)("deliberate" falsehoods); *Cummings v. HPG Intern., Inc.,* 244 F.3d 16 (1st Cir. 2001. *Compare Omitrus Merging Corporation v. Illinois Tool Works, Inc.*, 256 Ill. App. 3d 31, 628 N.E.2d 1165 (1994).

Classes: Unenforceable Exclusions from Liability

- **Personal injury or death:** Unenforceable in various jurisdictions. Under the UCC, limitation of consequential damages for injury to the person in the case of consumer goods is considered **prima facie unconscionable***.
- There also are issues with limitations for personal injury or death in **cross-border** agreements. Such clauses or the application of a general limitation clause to exclude such damages from liability are frequently prohibited by statute or regulations in other jurisdictions.**

*UCC § 2-719(3). See note on "unconscionability" below.

** *E.g.,* UK Unfair Contract Terms Act 1977, prohibiting an exclusion of liability for death or personal injury; UK Unfair Terms in Consumer Contracts Regulations 1999; Directive Concerning Liability for Defective Products (Product Liability Directive) [85/374/EEC], Arts. 9 and 12.

Classes: Unenforceable Exclusions from Liability

- **NB California**: Civil Code Section 1668: "All contracts which have for their object, directly or indirectly, to exempt anyone from responsibility for his own fraud, or willful injury to the person or property of another, or violation of law, whether willful or negligent, are against the policy of the law."*

**See* Cal. Civ. Code § 1668 ; *Farnham v. Superior Court*, 60 Cal. App.4th 69 (1997)(Section 1668 permits exclusion of ordinary negligence unless there is a special public interest or another statute forbids it); La. Civ. Code Ann. art. 2004; *Valhal Corp. v. Sullivan Associates, Inc.,* 44 F.3d 195 (3d Cir. 1995).

Classes: Unenforceable Exclusions from Liability

Form of General Savings Clause:

"NOTWITHSTANDING ANY CONTRARY PROVISION OF THIS AGREEMENT OR FAILURE OF THE ESSENTIAL PURPOSE OF ANY REMEDY, AND TO THE FULLEST EXTENT NOT PROHIBITED BY APPLICABLE LAW:"*

* *See* UCC § 2-719(2)(" Where circumstances cause an exclusive or limited remedy to fail of its essential purpose, remedy may be had as provided in this Act").

Classes: Unenforceable Exclusions from Liability

Form of Specific Savings Clause:

"NOTWITHSTANDING [CLAUSE _____ HEREOF (INDEMNIFICATION)] OR ANY OTHER PROVISION OF THIS AGREEMENT TO THE CONTRARY, NEITHER PARTY EXCLUDES OR LIMITS ITS LIABILITY CAUSED BY ITS OWN NEGLIGENCE FOR DEATH OR BODILY INJURY OR DAMAGE TO PHYSICAL PROPERTY, OR FOR ITS OWN FRAUD OR ILLEGAL OR UNLAWFUL ACTS, TO THE EXTENT THAT ANY SUCH EXCLUSION OR LIMITATION OF SUCH LIABILITY OTHERWISE WOULD BE VOID, PROHIBITED OR UNENFORCEABLE UNDER APPLICABLE LAW."

Classes: Alternatives to Exclusion from Liability

Alternatives to the Consequential Damages Exclusion:

(1) As a tactical alternative: propose an exclusion of liabilities for "**speculative or remote**" or "**unforeseeable**" damages rather than consequential damages per se. This is a ruse but can be effective.

(2) As a tactical alternative: require the breaching party to **indemnify and hold harmless** the plaintiff from such claims and provide that the indemnification is not subject to the consequential damages limitation [discussed below].

(3) Consider **deal-specific carve-outs** for claims involving known third party agreements or other identified potential losses [discussed below].

Classes: Exclusion of All Liabilities

- **Example: "**Company shall not be liable for any **direct**, indirect, incidental, special, consequential, exemplary, punitive or any other damages or losses of any kind or nature, whether in contract, tort (including negligence), products or strict liability or any other form of action…"
- Under the "hogs get slaughtered" doctrine, exclusion of all liabilities of any kind - including direct damages - can render a contract illusory and unenforceable, since the party can unilaterally discontinue performance at any time and breach with impunity.*

**E.g., Innovate Tech. Solutions, L.P. v. Youngsoft, Inc.,* 418 S.W.3d 148, 152-153 (Tex. App. 2013). *See generally Stein v. Paradigm Mirasol, LLC*, 586 F.3d 849, 858 (11th Cir. 2009); *Tractebel Energy Mktg. v. AEP Power Mktg*., 487 F.3d 89, 109-110 (2d Cir. 2007).

Limitation of Causes - Carve-Outs from Limitation of Liability

LIMITATION BASED ON CAUSES OF DAMAGES:
CARVE-OUTS FROM LIMITATION

Carve-Outs from Limitation of Liability

Case Study: Software company M licenses its software to Licensee for a flat fee of $100,000 per year. Licensee has the unlimited right to use the software for its own internal use. Licensee is expressly required under the contact to fully indemnify M for any breach of contract and for any violation of M's intellectual property rights. The contract also has a standard consequential damages exclusion, with a single carve-out for violation of the confidentiality provision.

Licensee redistributes the software to various third parties on a large scale in violation of the contract, resulting in huge losses of anticipated sales by M. M sues Licensee for breach of contract, IP infringement and indemnification.

What is the outcome?

Carve-Outs from Limitation of Liability

Common for parties expressly **carve-out** certain types of obligations and breaches as **exceptions** to the limitation of liability clause - in particular to the general consequential damages exclusion - due to their material nature and for their in terrorem effect.

This results in **unlimited liability** for these obligations and breaches subject to any cap [if any] on the amount of such damages.

These exceptions can include the following examples:

- Breach of **confidentiality and non-use obligations** for the confidential information of the other party [Alt: but not third parties]
- Gross negligence or willful misconduct

Carve-Outs from Limitation of Liability

- **Indemnification** obligations
- Infringement or misappropriation of intellectual property rights of the other party. The carve-out can be confined to (i) **willful infringement or misappropriation** of the IP rights to the other party [or any third party] or (ii) other intentional breaches of IP provisions of the contract.
- Breach of any **data protection** or **privacy** laws or obligations
- Fraud or fraudulent misrepresentation
- Bad faith
- Death or personal injury

Carve-Outs from Limitation of Liability

- Violations of [statutory][applicable] law
- Any **liquidated damages** provisions, which by definition can conflict with limitation of liability clauses.

Carve-Outs from Limitation of Liability

- Consider also **deal-specific** for known third party contracts or other known potential claims. This can be a flat carve-out for categories of losses such as (1) epidemic failure of product warranties, (2) willful failure to manufacture or deliver goods, (3) products liability for third party claims, or (4) lost profits.
- The carve-out can also limited by a **capped** amount, with any excess subject to the general limitation of liability.

Carve-Outs from Limitation of Liability

Example - Deal Specific Carve-Out by Category:

"NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL….DAMAGES OR LOSSES, **PROVIDED THAT** THE FOREGOING LIMITATION SHALL NOT BE APPLICABLE TO [THIRD PARTY] [CUSTOMER] [SUBDISTRIBUTOR] CLAIMS ARISING FROM OR RELATING TO (i) THE MATERIAL BREACH BY MANUFACTURER OF [X] PRODUCT WARRANTY OR (ii) ANY FAILURE OF MANUFACTURER TO DELIVER [Y] PRODUCT UNITS IN ACCORDANCE WITH SCHEDULE [Z]."

Carve-Outs from Limitation of Liability

Example - Deal Specific Carve-Out with Caps:

"[General consequential damage exclusion]; PROVIDED THAT SELLER SHALL BE LIABLE FOR ANY CONSEQUENTIAL OR INDIRECT OR SPECIFIC DAMAGES ARISING FROM DIRECT OR THIRD PARTY CLAIMS BASED ON ANY EPIDEMIC FAILURE OF THE PRODUCT, TO THE EXTENT SUCH DAMAGES IN THE AGGREGATE DO NOT EXCEED $____,000,000 IN ANY TWELVE-MONTH PERIOD".

Special Case - Indemnification Issues

Threading the Needle on Indemnification Obligations - Which has Priority?

- Critical to determine the **priority** of indemnification and limitation of liability clauses and to **coordinate** and "thread the needle" on those clauses. This can require a number of strategic decisions.
- Both clauses usually have "notwithstanding any contrary provision" language.

Red Flag - Indemnification Issues

Example: Limitation of Liability Priority:

"NOTWITHSTANDING ANY CONTRARY PROVISION OF THIS AGREEMENT, **INCLUDING** SECTION _____ (INDEMNIFICATION)"

- Contractual "Death Star": **Wipes out** any indemnification for excluded or limited liabilities, including consequential damages.
- **Imposes a cap** on the total amount of the indemnification obligation notwithstanding any language to the contrary in the indemnification clause.

Red Flag - Indemnification Issues

Example: Indemnification Priority:

"NOTWITHSTANDING ANY CONTRARY PROVISION OF THIS AGREEMENT, **OTHER** THAN SECTION _____ (INDEMNIFICATION)"

- If the indemnification clause has priority and includes "any and all claims" - or the indemnity includes "breaches" of the contract - **then this carve-out can entirely override and wipe out the limitation of liability clause [including the consequential damages exclusion].**
- This is especially a problem when both **direct and third party claims** are covered by the indemnification clause.

Red Flag - Indemnification Issues

Example: Indemnification Priority:

- It is also possible to argue that the **exclusive remedies** section of an indemnification clause overrides the limitation of liabilities clause as to the subject matter of the indemnification provisions. If there is an exclusive remedies section, the indemnitor should consider the following type of proviso:

  " [Exclusive remedies]; provided however that Section ____ (Limitation of Liabilities) and the exclusions and limitations set forth therein shall be applicable to any obligation of Indemnitor hereunder with respect to any Indemnified Matters."

Red Flag - Indemnification Issues

Compromise: Indemnification Priority for Third Party Claims Only:

"NOTWITHSTANDING ANY CONTRARY PROVISION OF THIS AGREEMENT, OTHER THAN SECTION _____ (INDEMNIFICATION) IN THE CASE OF UNAFFILIATED THIRD PARTY CLAIMS"

- Common issue in negotiations will be whether indemnification for third party claims representing consequential damages are to be excluded from limitation of liabilities. Rationale is that the indemnitee should indemnified without regard to the character of the damages in the third party action.

Red Flag - Indemnification Issues

Compromise: Limitation of Liability Priority - Cap on Liability:

“NOTWITHSTANDING ANY CONTRARY PROVISION HEREOF, INCLUDING SECTION ___ (INDEMNIFICATION), COMPANY SHALL NOT BE REQUIRED TO INDEMNIFY, HOLD HARMLESS OR DEFEND ABC OR OTHER ABC INDEMNITEES UNDER THIS AGREEMENT TO THE EXTENT THE AGGREGATE AMOUNT OF ALL CLAIMS DURING [TIME PERIOD] EXCEEDS $_____ [CAP]; [EXCLUDING OR SEPARATE CAP FOR CERTAIN CLASSES OF INDEMNIFICATION] [EXCLUDING OR SEPARATE CAP FOR ALL DEFENSE COSTS]."

Red Flag - Priority Issues

Data Point on "Notwithstanding" Language:

- Note that if you intend in a limitation of liability clause to have its terms apply "notwithstanding any contrary provision", this qualifier should apply to **both any exclusions of liabilities** such as consequential damages **and any other general limitation of liabilities** such as caps on the amount of damages.
- In such case use as a **preamble** to the **entire** limitation of liabilities clause - with any other qualifiers - rather than only to consequential damages subsection - a very common error.

Limitation of Amount

LIMITATION OF AMOUNT OF DAMAGES

Limitation of Amount

Limitation of liability clauses will commonly include a limitation on the **amount of liabilities** to which a party is subject (a "**cap**"), in one or more of the following forms:

(1) As a multiple of the contract price or fees or royalties payable under the contract:

"The total liability under the contract shall not exceed 10% of the acquisition price" or "the total fees paid to Company by ABC in the aggregate within the 12 month period preceding the initial event which gave rise to the liability".

Limitation of Amount

(2) As a lump sum:

"The total liability under the contract shall not exceed $ X."

(3) A combination of the above:

"The total liability under the contract shall not exceed the [greater][lesser] of $ X or 10% of the acquisition price".

- There are numerous variations used on the formula for caps in US limitation of liabilities clauses, including the use of subcaps for specific classes of liability.

Limitation of Amount

- Caps on liabilities which are **unreasonably low** or otherwise do not bear a rational relationship to the terms of the deal - especially in consumer contracts - can be disregarded on grounds of **unconscionability**.*

*UCC § § 2-302, 2-719(3). *See, e.g.,* Cal. Civ. Code § 1670.5 ; *Lucier v. Williams,* 841 A. 2d 907 (NJ App. 2004). *See MyPlayCity, Inc. v. Conduit Ltd.*, 2013 U.S. Dist. LEXIS 6029 (S.D.N.Y., Jan. 11, 2013)($5,000 cap upheld).

Note on Unconscionability: Whether a limitation clause is unconscionable is a question of law to be determined by the court, and the specific standards for finding unconscionability depend on the number of factors. *E.g., NEC Technologies, Inc. v. Nelson*, 267 Ga. 390, 391-92, 478 S.E.2d 769 (1996). In this context the overriding principle is one of the prevention of oppression and unfair surprise and not of disturbance of allocation of risks because of superior bargaining power. Official Comment to UCC § 2-302, sec. 1.

Some courts distinguish between procedural unconscionability [oppression and surprise unequal bargaining power] and substantive unconscionability [overly harsh or unfairly one-sided provisions]. *Little v. Auto Stiegler, Inc.*, 29 Cal. 4th 1064 (Cal. 2003). Formulations of the rule include an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party [*Williams v. Walker-Thomas Furniture Co.*, 350 F.2d 445 (D.C. Cir. 1965)] where "one party has been misled as to the nature of the bargain, where there appears to have been a severe imbalance in bargaining power, or where specific terms appear 'outrageous'" [*County Asphalt, Inc. v Lewis Welding & Engineering Corp.,* 444 F.2d 372 (2d Cir. 1971)]; or where fine print or convoluted language is used in the contract [*John Deere Leasing Co. v. Blubaugh*, 636 F. Supp. 1569, 1573 (D. Kan. 1986)].

Limitation of Amount

Example (1) - Cap based on fees over time:

"IN NO EVENT SHALL THE TOTAL LIABILITY OF COMPANY OR ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED [_____ PERCENT OF] THE TOTAL FEES ACTUALLY PAID TO COMPANY BY CUSTOMER IN THE AGGREGATE DURING THE 12 MONTH PERIOD PRECEDING THE INITIAL EVENT WHICH GAVE RISE TO THE LIABILITY."

Limitation of Amount

Example (2) - Cap based on fees - value of contract over the term:

"IN NO EVENT SHALL THE TOTAL LIABILITY OF COMPANY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED (i) THE TOTAL FEES ACTUALLY PAID TO COMPANY BY CUSTOMER IN THE AGGREGATE DURING THE PERIOD PRECEDING THE INITIAL EVENT WHICH GAVE RISE TO THE LIABILITY ("INITIAL PERIOD"), **PLUS** (ii) THE AVERAGE MONTHLY FEE DURING THE INITIAL PERIOD MULTIPLIED BY THE NUMBER OF REMAINING MONTHS UNDER THE TERM OF THE AGREEMENT".

Limitation of Amount

Example (3) - Cap based on fees plus a total cap:

"IN NO EVENT SHALL THE TOTAL LIABILITY OF COMPANY OR ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL FEES ACTUALLY PAID TO COMPANY BY CUSTOMER IN THE AGGREGATE DURING THE 12 MONTH PERIOD PRECEDING THE INITIAL EVENT WHICH GAVE RISE TO THE LIABILITY; PROVIDED FURTHER THAT IN NO EVENT SHALL THE MAXIMUM LIABILITY OF THE COMPANY FOR ALL CLAIMS ARISING OUT OR RELATED TO THIS AGREEMENT EXCEED _____ MILLION DOLLARS (US $___,000,000) IN THE AGGREGATE."

Limitation of Amount

Example (4) - Total cap:

"IN NO EVENT SHALL THE TOTAL LIABILITY OF COMPANY OR ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED _____ MILLION DOLLARS (US $____,000,000) IN THE AGGREGATE."

Limitation of Amount

Example (5) - Total cap with shared excess liabilities:

"THE COMPANY SHALL BE LIABLE FOR ALL CLAIMS ARISING OUT OF OR RELATED TO THIS AGREEMENT TO THE EXTENT NOT IN EXCESS OF _____ MILLION DOLLARS (US $___,000,000) IN THE AGGREGATE; AND THEREAFTER COMPANY SHALL BE ONLY BE LIABLE FOR THE PAYMENT OF _____ PERCENT (_____%) OF ALL EXCESS AMOUNTS OF SUCH CLAIMS."

Limitation of Amount

Example (6) - Total cap with declining amount:

"IN NO EVENT SHALL THE TOTAL LIABILITY OF COMPANY OR ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED _____ MILLION DOLLARS (US $___,000,000) IN THE AGGREGATE, AS REDUCED MONTHLY COMMENCING ON _____, 2015 ON A PRO RATA BASIS FOR THE REMAINDER OF THE TERM."

Limitation of Amount

Example (7) - Subcaps - Deal Based

"(i) IN NO EVENT SHALL THE LIABILITY OF MANUFACTURER FOR ANY CLAIM ARISING OUT OF OR RELATING TO ANY PATENT OR LATENT **DEFECTS IN THE DESIGN, MATERIALS OR WORKMANSHIP** OF THE PRODUCTS EXCEED THREE MILLION DOLLARS (US $3,000,000) IN THE AGGREGATE.

(ii) IN NO EVENT SHALL THE LIABILITY OF MANUFACTURER FOR ANY CLAIM ARISING OUT OF OR RELATING TO ANY **FAILURE TO MANUFACTURE AND DELIVER** TO ABC THE MINIMUM QUANTITIES OF PRODUCT UNITS IN ANY CALENDAR YEAR DURING THE TERM EXCEED TWO MILLION DOLLARS (US $2,000,000) IN THE AGGREGATE."

Limitation of Amount

Example (8A) - Subcap for Intellectual Property - Primary Clause

"IN NO EVENT SHALL THE LIABILITY OF [MANUFACTURER][EITHER PARTY] FOR ANY CLAIM ARISING OUT OF OR RELATING TO ANY BREACH OF SECTION _____ (INTELLECTUAL PROPERTY WARRANTIES) OR SECTION ____ (INTELLECTUAL PROPERTY INDEMNIFICATION) EXCEED FIVE MILLION DOLLARS (US $5,000,000) IN THE AGGREGATE; [exclusions]."

Limitation of Amount

Example (8B) - Exclusions for Subcap for Intellectual Property - Willful Infringement

"; PROVIDED HOWEVER THAT (A) IN THE CASE OF ANY CLAIM OF WILLFUL INFRINGEMENT OR MISAPPROPRIATION, OR OTHER INTENTIONAL BREACH OF THE FOREGOING SECTIONS [SHALL NOT EXCEED FIFTEEN MILLION DOLLARS (US $15,000,000) FOR EACH CLAIM OR RELATED CLAIMS] **or** [SHALL NOT BE SUBJECT TO ANY LIMITATION OR CAP].

Limitation of Amount

Example (8C) - Exclusions for Subcap for Intellectual Property - Costs of Defense

"; PROVIDED HOWEVER THAT…(B) THE FOREGOING CAPS SHALL NOT INCLUDE ANY COSTS OF DEFENSE AGAINST ANY SUCH CLAIMS (INCLUDING BUT NOT LIMITED TO ATTORNEY'S FEES AND COSTS, EXPERT'S FEES AND OTHER EXPENSES OF LITIGATION), WHICH COSTS OF DEFENSE SHALL NOT BE SUBJECT TO ANY LIMITATION OR CAP."

Limitation of Amount

Example (9) - Subcap for Indemnification

"NOTWITHSTANDING ANY CONTRARY PROVISION HEREOF, THE INDEMNIFICATION OBLIGATIONS OF COMPANY IN SECTION _____ SHALL NOT BE APPLICABLE TO THE EXTENT THAT THE AGGREGATE AMOUNT OF ALL PAYMENTS MADE OR INCURRED BY COMPANY TO **INDEMNIFY AND DEFEND** ABC AND OTHER ABC PERSONS FOR ALL CLAIMS **UNDER SECTION _____ (INDEMNIFICATION OBLIGATIONS)** EXCEED ___ MILLION DOLLARS (US $____,000,000) [EXCLUDING CERTAIN CLASSES OF INDEMNIFICATION] [EXCLUDING ALL DEFENSE COSTS]."

Limitation of Amount

Example (9) - Subcap for Indemnification

- **Defined Terms**: The terms “indemnify”, “hold harmless” and “defend” have distinct and separate meanings under the rules governing indemnification provisions. Use a collective definition for such terms such as:

  “Each party agrees to fully indemnify and hold harmless and defend (collectively ‘indemnify’ or ‘indemnification’ or any variation thereof)”.

- **No Cap for Costs:** Failure to define terms can result in a subcap limiting only the obligation to **indemnify** and not the separate obligation to **defend**, resulting in unlimited liability for defense costs.

Limitation of Amount

Example (9) - Subcap for Indemnification

Example of **flawed** cap - Indemnity only:

“NOTWITHSTANDING ANY CONTRARY PROVISION HEREOF, INCLUDING SECTION ___ (INDEMNIFICATION), COMPANY SHALL NOT BE REQUIRED TO **INDEMNIFY** ABC UNDER THIS AGREEMENT TO THE EXTENT THE AGGREGATE AMOUNT OF ALL CLAIMS EXCEEDS $_____ [CAP]."

OTHER MATTERS

Alternative Sources of Limitation of Liabilities

- **Liquidated damage clauses**
- **Contractual statutes of limitation**
- **Disclaimers and Time Limitations for Warranty Claims:** Note that disclaiming or limiting the scope of warranties or covenants - such as implied warranties of merchantability - or imposing a time period [such as 24 months from closing] for bringing any warranty claims are also a form of limitation of liability.*

**See* UCC § 2-316(2).

Other Issues

- **Equitable relief:** The limitation of liability clause does not prevent a court from granting equitable relief such as specific performance. Specific performance or other equitable remedies should be expressly excluded if intended.*
- **Exclusive Remedy:** At least in the case of contracts subject to the UCC, state that (i) the limitation of liabilities section applies notwithstanding any contrary provision of the contract and (ii) sets forth the sole and exclusive rights and remedies of each party for any claims of liability by the other party.**

* *E.g., Vacold LLC v. Cerami*, 545 F.3d 114, 130-131 (2d Cir. 2008).

**UCC § 2-719(1)(b)("expressly agreed to be exclusive, in which case it is the sole remedy").

Other Issues

- **Scope:** Any exclusion or limitation should apply to not only to claims or liabilities per se but also to damages and losses incurred by the other party.
- **Cumulative Damages:** As in the case of indemnification, the best practice is for any cumulative damages provision to be expressly made subject to the limitation of liabilities clause.
- **Severability:** The limitation of liability clause should have additional severability language in the body of the clause: "to the fullest extent not prohibited by applicable law".
- **Choice of law and forum** can be critical to enforcement of limitation of liability clause.

Other Issues

- **Conspicuous**: Limitation of liability clauses should be conspicuous to limit claims of surprise or oppression or other forms of unconscionability. The general practice is to use CAPS for the clause.*

*Note that under the Uniform Commercial Code conspicuous is **not** a statutory requirement for a limitation of remedies clause in a sale of goods contract; it is only a requirement for a disclaimer of warranties. UCC § § 2-316, 2-719. Under the UCC, a term is considered conspicuous when it is "so written, displayed, or presented that a reasonable person against which it is to operate ought to have noticed it." UCC § 1-201(b)(10).

Use of CAPS is not fool-proof. "Lawyers who think their caps lock keys are instant 'make conspicuous' buttons are deluded. In determining whether a term is conspicuous, we look at more than formatting. A term that appears in capitals can still be inconspicuous if it is hidden on the back of a contract in small type. *See, e.g., Sierra Diesel*, 890 F.2d at 114. Terms that are in capitals but also appear in hard-to-read type may flunk the conspicuousness test. *See, e.g., id.; Lupa v. Jock's*, 131 Misc. 2d 536, 500 N.Y.S.2d 962, 965 (N.Y. City Ct. 1986). A sentence in capitals, buried deep within a long paragraph in capitals will probably not be deemed conspicuous. Formatting does matter, but conspicuousness ultimately turns on the likelihood that a reasonable person would actually see a term in an agreement. Thus, it is entirely possible for text to be conspicuous without being in capitals." *Am. Gen. Fin., Inc. v. Bassett (In re Bassett)*, 285 F.3d 882, 886 (9th Cir. 2002)(emphasis added).

Other Issues

- **Third Party Beneficiaries:** Any "third party beneficiaries" clause should have carve-outs for (i) third party indemnitees under the indemnification clause and (ii) any third parties [such as "affiliates"] who are express beneficiaries of the limitation of liabilities clause.
- **Survival:** The limitation of liabilities clause should be expressly included in any survival of termination clause

Tab 6

Protecting Your IP
Tips for In-House Counsel

Moderator: Ira Kotel, Partner, Dentons

Panelists:

Annemarie Brennan, Vice President & Associate General Counsel, Sivantos Group

Deidra Gold, Executive Vice President & General Counsel, Wolters Kluwer

Heather Khassian, Counsel, Dentons

November 29, 2016

Protecting Your Brand
How companies manage brands globally

Brand Management in Modern Global Economy

- Pace of branding/advertising is much faster
- Companies have instantly connection with their customers, suppliers, and distributors.
  - Many companies have completely internet based presence (no print materials, no trade shows, etc)
- Consumers have voluminous information available that corporations need to continually assess
- "Third party" sources are taking a critical role
  - (e.g. Amazon reviews, yelp, Angie's list)

Global Brand Considerations

- Filing a single trademark globally is expensive
  - Estimates for a single mark, single class, in about 100 countries globally to be approximately $500k
    - Additional classes, variations on a single mark, can cause exponential rise in fees
- Managing trademarks globally is expensive
  - Policing marks globally requires man power
  - Requires folks culturally sensitive to issues in regions of concern

Non-competes

Favored by some and hinder other industries

Non-competes

- Certain industries favor them; others have significant rebellion against them
- Remain generally enforceable in most jurisdictions
  - Not generally enforceable in certain states (e.g. California, Montana, North Dakota, Oklahoma)
- Remain a valid means of protecting certain intellectual property with certain employees

Non-compete statistics

- Survey of 500 S&P 1500 companies CEO contracts. most of the CEO contracts (80%) had 1 or 2-year covenants not to compete (CNCs)
  - 89% of CNCs prohibited CEOs from working for a competitor, but only 25% prohibited CEOs from financing one
  - almost 40% of CNCs barred CEOs from working anywhere where the company had operations
  - 75% of CEO contracts barred them from soliciting companies' employees, but only 50% barred CEOs from soliciting clients
  - almost 90% of the contracts had a non-disclosure clause
  - more than half of CNCs were triggered by *any* departure of the CEO, whether voluntary or not

Why trade secrets matter

- Companies are placing more and more of their value in intangible assets
- Misappropriation of trade secrets is on the rise
  - 25%+ of companies reported theft of trade secrets in 2014
  - The way trade secrets are stored today makes misappropriation much easier
- Work force is highly mobile
  - In 2012, average time spent with any single employer for all employees is 4.6 years
- Patents are becoming less valued, especially by certain technology sectors
  - Trade secrets are becoming more highly valued in response
- Jury awards related to trade secret misappropriation are high

Infringement allegations
Addressing them, especially those with global implications

Infringement Allegations

- Infringement allegations oftentimes have global implications
  - Trademarks used in various regions
  - Product lines related to patents in various jurisdictions
  - Expenses increase exponentially!

Data breach crises strategies

How strategies differ by region and industry

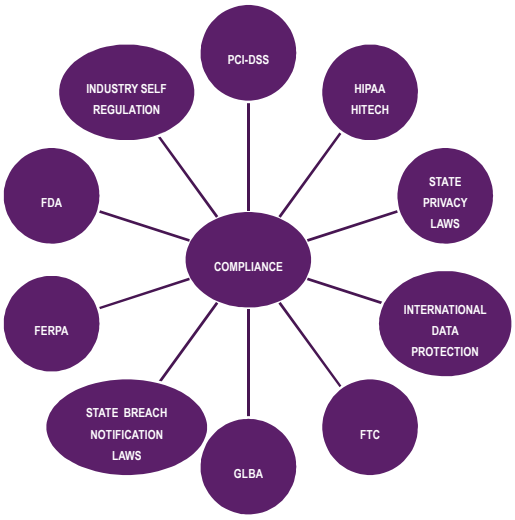
Breach is Predominantly Determined by State Laws

- 47 states, D.C., & U.S. territories
- Definitions differ for what constitutes “personal information”
- Some laws require notification of residents based upon “unauthorized access”
- Some require a risk of harm analysis to determine whether notification is required
- Many states require notice to the State Attorney General or specific agency
- Notice within a defined timeframe, but these timeframes can vary
- Limited precedent

What is a Data Breach? (That may trigger state notification laws)

- Unauthorized access to and acquisition of specific types of information associated with a named individual
  - SSN
  - Driver's license number
  - Credit card number
  - Bank account Information
  - information that identifies an individual and relates to:
    (i) the physical or mental health or condition of the individual;
    (ii) the provision of health care to the individual; or
    (iii) payment for the provision of health care to the individual.

Compliance is Complex



Dealing with patent trolls

Global licensing issues and industry coordinated efforts across borders

Dealing with patent trolls

- 60%+ of all patent infringement suits filed by NPE
  - In some sectors the number is as high as 90% (high tech)
- Trend to settle for lower amounts of money, but with more defendants
  - But some companies have taken a never settle approach
- PTAB filings up for inter partes review

Unified Responses

- Industries joining forces and aligning
  - Offensive measures
  - Defensive measures
- "NPE Insurance"

Best advice

Based on personal experience for developing global IP strategies

Best Advice

- Our panelist share their best advice
  - (a.k.a. "I wish I had known…")

Thank you!