GTC

LAWYERS + STRATEGISTS

GTC Data Privacy & Security Training

November 3, 2017

Hosted by

juniper® NETWORKS

SPECIAL THANKS TO ....

EMILY CHANG
ASSISTANT GENERAL COUNSEL, DIRECTOR

GTC DATA PRIVACY & SECURITY GROUP

David Bender

Brent Bliven

Sayoko Blodgett-Ford

Thomas Hemnes

Jennifer Heisler Lavalley

Grace Lee

Rick Olin

Stephen Pakan

Laila Paszti

Mirjam Supponen

gtclawgroup.com

PLEASE GIVE YOUR QUESTION CARDS TO:

Laila Paszti

Mirjam Supponen

AGENDA

9am-9:15am - Announcements and Kickoff

9:15am - 10:15am Mergers & Acquisitions – Data Privacy & Security (Panel #1)

Jon Adams, Senior Privacy Counsel, LinkedIn
Rocco Grillo, Executive Managing Director, Cyber Resilience Leader, Stroz Friedberg/Aon
Sayoko Blodgett-Ford, Member & Chief Privacy Officer, GTC Law Group

10:15am - 11am Beyond the Basics: Recent Developments in Global Data Privacy & Security

David Bender, Special Counsel, Data Privacy, GTC Law Group and Distinguished Fellow, Ponemon Institute

11am - 11:10am *BREAK*

11:10am - 12:10pm Vendor Risk Management – Data Privacy & Security (Panel #2)

Sherry Ryan, CISO, Juniper
Tanya O'Connor, Director, Information Security, Arcadia Healthcare Solutions
Gary Roboff, Senior Advisor, Santa Fe Group - Shared Assessments
Rick Olin, Shareholder, CIPP/US, GTC Law Group

12:10pm - 12:30pm Closing

JON ADAMS
Senior Privacy Counsel

Part of a team that oversees LinkedIn's privacy and data protection compliance program.

Certified Information Privacy Professional (CIPP/US)

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

- Privacy and technology transactions

SIDLEY AUSTIN LLP
SIDLEY

- Product, transactional, and compliance counseling relating to privacy, data protection, cybersecurity, and intellectual property matters.

- Federal Trade Commission, Bureau of Consumer Protection

DAVID BENDER
Special Counsel - Data Privacy

GTC
LAWYERS + STRATEGISTS

Ponemon INSTITUTE

Ponemon Institute Distinguished Fellow

WHITE & CASE

Co-founded the Privacy practice, and founded the IP practice, at White & Case, and headed that firm's Privacy practice. Work included privacy audits to bring corporations into global compliance, vetting proposed conduct of multinationals to ascertain compliance with pertinent privacy laws, and advising on cross-border data transfer.

AT&T

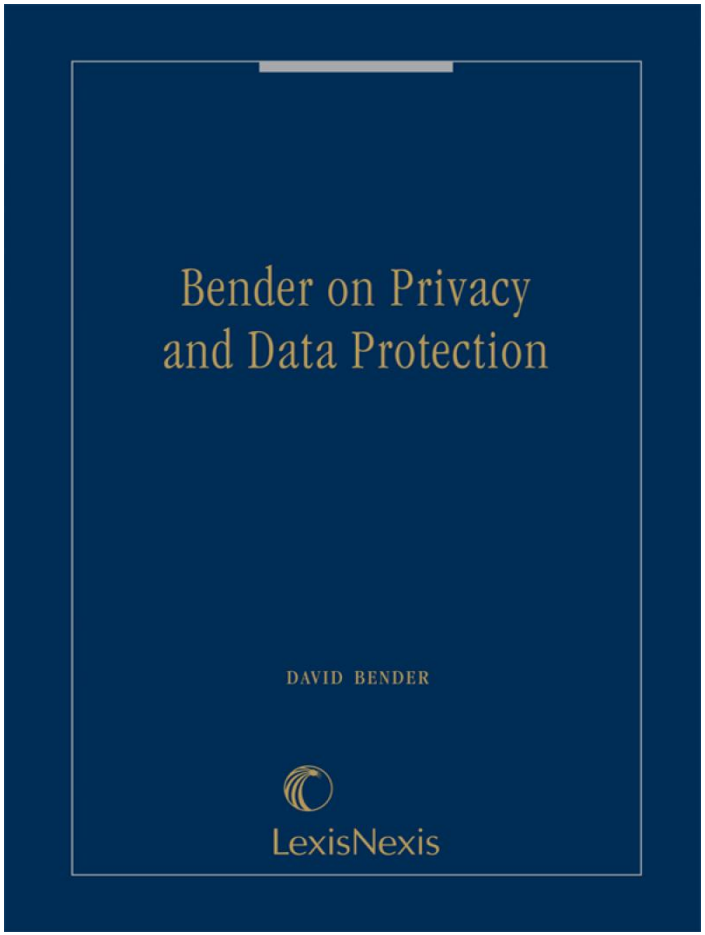
Served in-house at AT&T for 10 years, responsible for all IP litigation brought by or against any Bell System company during the latter half of that period.

UNIVERSITY OF HOUSTON FOUNDED 1927

PACE UNIVERSITY

Teaches Privacy Law at the University of Houston and Pace University.

LexisNexis



Bender on Privacy and Data Protection

by David Bender (Author)

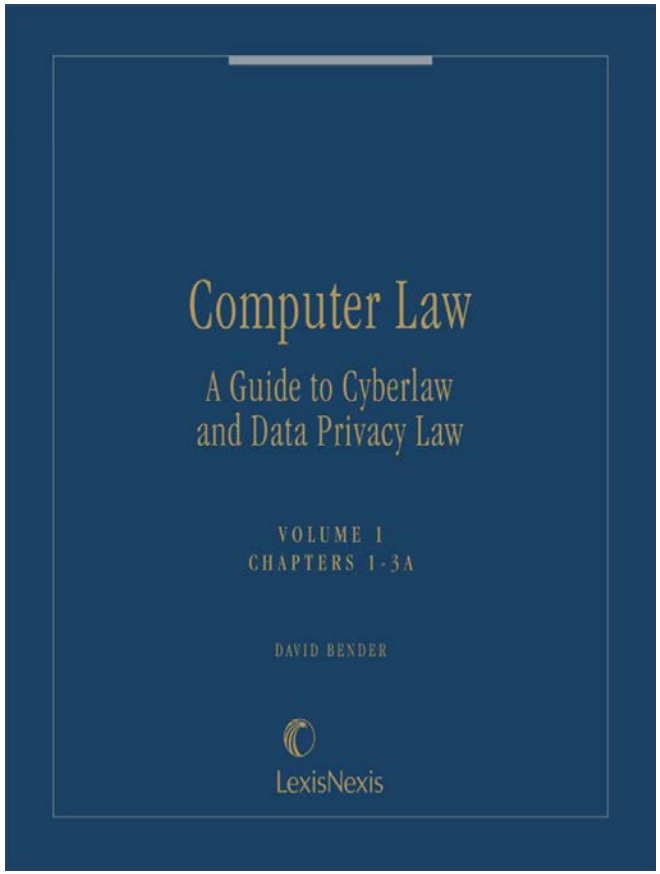
Publisher: LexisNexis

Select a format

	Price	QTY
eBook :mobi ISBN: 9780769890630 Published: October 09, 2014 IN STOCK	$268.00	- 1 +
eBook :epub ISBN: 9780769890630 Published: October 09, 2014 IN STOCK	$268.00	- 1 +

https://store.lexisnexis.com

LexisNexis



Computer Law: A Guide to Cyberlaw and Data Privacy Law

by David Bender (Author)
Publisher: Matthew Bender
Frequency: (2 issues)

Print Book :6 Volumes; Looseleaf updated twice annually
ISBN: 9780820510682
IN STOCK

eBook :epub
ISBN: 9781579113940
IN STOCK

eBook :mobi
ISBN: 9781579113940
IN STOCK

https://store.lexisnexis.com

SAYOKO BLODGETT-FORD
Member & Chief Privacy Officer

GTC
LAWYERS + STRATEGISTS

Certified Information Privacy Professional (CIPP/US)

- Boston College Law School – Adjunct
- Teaches Privacy Law & Mobile App Development – Legal

- Served as General Counsel of Tetris Online, Inc.

- Served as Senior Manager of the Intellectual Property Group at Nintendo of America Inc.

- Court Appointed Arbitrator - Hawai'i State District Court

Rocco Grillo

STROZ FRIEDBERG
an Aon company

Executive Managing Director/ Cyber Resilience Leader

Oversees and supervises Stroz Friedberg's global Cyber Resilience business.

Advises clients, including boards and executive management on a range of cybersecurity issues across all industries

Internationally recognized expert in the field of Information Security and Incident Response investigations

protiviti®
Face the Future with Confidence

- Served as Managing Director and Global Leader of Protiviti's Incident Response & Forensics Investigations practice.

FINANCIAL SERVICES ISAC

- Affiliate Board Advisor for FS-ISAC, assisting in the development of annual tabletop exercises to assess the readiness of financial institutions in the event of a cyber-attack.

TANYA O'CONNOR
Director, Information Security

arcadia HEALTHCARE SOLUTIONS

Strategic security and privacy planning/implementation and responding to customer privacy/security assessments.

Over 13 years of experience in IT security, accreditation, compliance, vulnerability assessments, remediation, monitoring and strategic cybersecurity planning and policy development.

ORACLE®

- Served as Compliance Manager and Security Lead at Oracle Corporation.

THE DEPARTMENT OF THE TREASURY 1789

- Former Information Systems Security Manager, U.S. Department of the Treasury.

DEPARTMENT OF THE NAVY UNITED STATES OF AMERICA

- Former Information Security Business Analyst and Information Assurance Governance Analyst, U.S. Navy.

Rick Olin
Shareholder

GTC
LAWYERS + STRATEGISTS

Certified Information Privacy Professional (CIPP/US)

- Served as Vice President, General Counsel and Secretary of TechTarget, Inc.
- Served as Senior Vice President of Corporate Development, General Counsel and Secretary at Workscape, Inc. (acquired by ADP, Inc.)
- Served as Vice President, General Counsel and Secretary of SpeechWorks International, Inc. (acquired by ScanSoft, Inc. and now Nuance Communications, Inc.)
- Served as Deputy Legal Counsel at Open Market, Inc.
- Former member of the business law section at Mintz, Levin in Boston.

GARY ROBOFF
Senior Advisor

SANTA FE GROUP

Payments, risk management, mobile financial services, and information management.

- Four decades of experience in financial services planning and management, including 25 years at JP Morgan Chase.
- Founder of Chase Merchant Services LLC (now Chase Paymentech).
- Led the development of pinned debit services at Chemical and Manufacturers Hanover.
- Former President and CEO of the New York Switch Corporation, (the NYCE ATM and Debit Network) and founder of its successor corporation (NYCE Corporation, now an affiliate of FIS)

SHERRY RYAN
IT Vice President and CISO

JUNIPER NETWORKS

Certified Information Security Manager (CISM) and Certified Information Systems Security Professional (CISSP)

- Served as CISO, Blue Shield of California
- Served as CISO, Hewlett-Packard
- IT Security, Safeway
- Global Information Security, Levi Strauss
- Member of the High Tech Crime Investigation Association (HTCIA) and the Information Systems Security Association (ISSA).

Data Privacy & Security in the News ...

Actually, every single Yahoo account got hacked in 2013

The Washington Post

Brian Fung October 3

All of Yahoo's 3 billion user accounts in 2013 were affected by its massive data breach — not the 1 billion accounts that were initially reported, the company said Tuesday.

The revised number vastly expands the scope of the historic hack, which had previously broken records as the world's largest data breach. The updated figure comes as the public is still reeling from back-to-back reports of data breaches at Equifax and the fast-food chain Sonic.

YAHOO!®

Google Hit With New Privacy Suit For Sharing Data With App Developers

DigitalNewsDaily

by Wendy Davis October 11, 2017

This latest complaint was brought by Minnesota resident Adam Gurno, who alleges that he purchased nine apps totaling more than $26 from the Google Play Store between 2012 and 2014. Gurno alleges that Google transmitted his name, email address and ZIP code to the developers without his consent.

Gurno quietly brought his class-action complaint last month in California state court. Google transferred the matter to federal court on Tuesday.

Privacy?

The world once laughed at North Korean cyber power. No more

By David E. Sanger and David D. Kirkpatrick | NEW YORK TIMES OCTOBER 15, 2017

While its track record is mixed, **North Korea's army of more than 6,000 hackers** is undeniably persistent, and improving, according to American and British security officials who have traced cyberattacks to the North.

When North Korean hackers tried to **steal $1 billion** from the New York Federal Reserve last year, only a spelling error stopped them.

AFP/GETTY IMAGES/FILE

Staffers at the Korea Internet and Security Agency in Seoul monitored cyberattacks that some blamed on North Korea.

T-Mobile website bug let hackers steal data with a phone number

engadget

Steve Dent, @stevetdent
10.11.17 in Security

Up until last week, a T-Mobile website had a serious security hole that let hackers access user's email addresses, accounts and a phone's IMSI network code, according to a report from *Motherboard*. Attackers only needed your phone number to obtain the information.

The security researcher who discovered the hole, Karan Saini from startup Secure7, notes that anyone could have run a script to **scrape the data of all 76 million T-Mobile users** and create a searchable database.

TripAdvisor subsidiary data breach hits up to 1.4 million customers

SC MEDIA by Tim Ring September 23, 2014

viator

tripadvisor

Viator was acquired by TripAdvisor, the world's largest travel site, for £122 million (US$ 200 million) last month – and TripAdvisor saw its NASDAQ shares slump 4 percent after the breach was disclosed, though they partially recovered later.

US-based Viator - which has a regional office in London - admitted late on Friday that criminals have hacked into some of its customers' payment card accounts and made unauthorised charges.

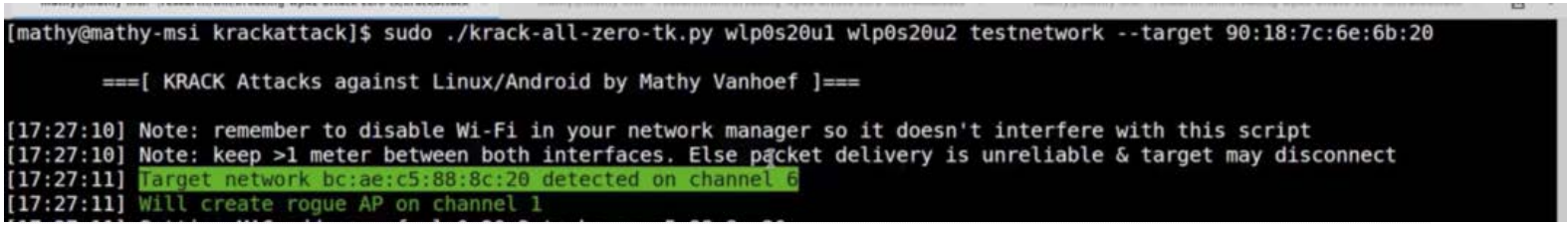
WPA2 security flaw puts almost every Wi-Fi device at risk of hijack, eavesdropping

ZDNet

By Zack Whittaker for Zero Day | October 16, 2017

The bug, known as "KRACK" for Key Reinstallation Attack, exposes a fundamental flaw in WPA2, a common protocol used in securing most modern wireless networks

This flaw, if exploited, gives an attacker a skeleton key to access any WPA2 network without a password. Once they're in, they can eavesdrop on your network traffic.



Canada proposes EU-like regulations for mandatory data breach-reporting

REUTERS

OCTOBER 3, 2017

Canada has proposed new regulations outlining how organizations, including financial firms, will report and record cyber-security breaches, assess potential harm, and notify affected individuals. The proposal, which aligns with EU data-protection rules that take effect next year, is intended to implement mandatory breach-reporting requirements described in the Digital Privacy Act of 2015

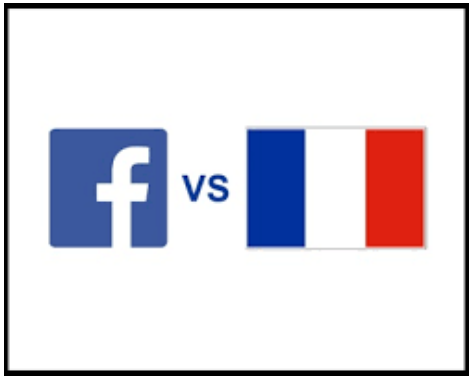
Facebook facing privacy actions across Europe as France fines firm €150k

theguardian

Samuel Gibbs
Tuesday 16 May 2017 16.23 BST

Facebook has been fined €150,000 (£129,000) by France's data protection watchdog and is being investigated by Belgium, the Netherlands, Germany and Spain for data privacy violations around the tracking of users and non-users and the use of user data for advertising.

The data regulators clubbed together to form a so-called contact group to analyse the changes Facebook made to its privacy policy in 2014. The French watchdog CNIL hit Facebook with the maximum fine possible at the point at which it started its investigation in 2014. As of October last year CNIL can now issue fines of up to €3m.



Facebook dealt setback by EU court adviser in privacy dispute

REUTERS

Julia Fioretti OCTOBER 24, 2017 / 11:57 AM

BRUSSELS (Reuters) - Facebook was dealt a setback on Tuesday when an adviser to the top European Union court said any data protection authority in the bloc had the power to take action against it for breaching privacy laws.

Facebook has its European headquarters in Ireland and has argued that only the Irish data protection authority has the power to police it for its processing of Europeans' data. Nonetheless other European privacy regulators, including the French, Belgian and German authorities, have taken action against the U.S. company.

Generally, opinions from court advisers tend to be followed by the Court's judges in a majority of cases. A final ruling should follow in the coming months.

THE
NATIONAL LAW REVIEW

An Irish Court Clouds the Future of EU Data Transfers: The Luck of the Model Clauses May Be Done

Friday, October 6, 2017

An Irish court has referred another case brought by Mr. Schrems against Facebook to the EU's top court, the Court of Justice of the European Union (the CJEU), to determine whether the standard (i.e., "model") contractual clauses drafted by the EU to provide an "adequate" level of protection when companies transfer personal data outside the EU ("model clauses") are compliant with the EU's laws on privacy.

Whole Foods suffers data breach in some stores

CNBC

Angelica LaVito
Published 5:33 PM ET Thu, 28 Sept 2017
Updated 7:27 PM ET Thu, 28 Sept 2017

Whole Foods, which was recently acquired by Amazon, suffered a data breach of credit card information used in taprooms and full table-service restaurants in some of the grocery chain's stores, the company said Thursday.

Whole Foods noted these venues use a different point-of-sale system than the main checkout systems. Credit cards used at those systems were not affected, the company said.

Millions caught in South Africa's 'worst data breach'

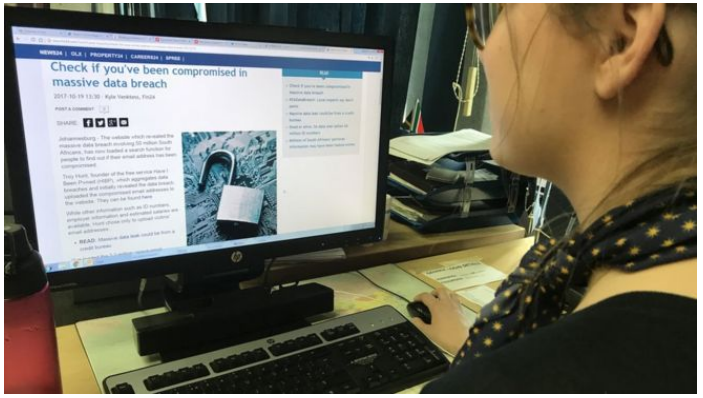
By Pumza Fihlani
20 October 2017 | Africa

BBC News, Johannesburg

Authorities in South Africa are investigating a data breach which has seen the personal details of more than 30 million citizens leaked on the internet - placing them at risk of identity theft.

The information contained in a 27GB file was discovered by Australia-based internet security expert Troy Hunt earlier this week.

It contains their names, full identity numbers, income, gender, employment history, contact numbers and even home addresses.



Governor Andrew M. Cuomo today announced the first-in-the-nation cybersecurity regulation to protect New York's financial services industry and consumers from the ever-growing threat of cyber-attacks will take effect on March 1, 2017. The final regulation requires banks, insurance companies, and other financial services institutions regulated by the Department of Financial Services to establish and maintain a cybersecurity program designed to protect consumers' private data and ensure the safety and soundness of New York's financial services industry.

NEW YORK STATE

Google right to be forgotten spat returns to Europe's top court

ars technica

KELLY FIVEASH (UK) - 11/24/2016, 11:30 AM

Google's dispute with France's privacy watchdog over a call to apply "right to be forgotten" rules globally to some Web links will be weighed by Europe's top court—three years after it told the ad giant to comply with an order to remove old, out of date, or irrelevant listings from its powerful search index, so long as they weren't found to be in the public interest.

French data regulator, the CNIL (Commission Nationale de l'Informatique et des Libertés), previously called on Google to globally delist certain search results. Last year, the multinational said it would appeal against CNIL's order, which included a €100,000 fine for failing to remove certain links from its global search results.

Supreme Court agrees to review Microsoft Ireland warrant case

The Washington Post By Orin Kerr October 16

The Supreme Court has agreed to hear the Microsoft Ireland warrant case. As regular readers know, this is the case on whether Microsoft has to comply with a search warrant obtained in the United States that orders Microsoft to retrieve customer files Microsoft has stored in Ireland.

Of course, the court already has pending *Carpenter v. United States*, a constitutional case on whether the Fourth Amendment protects historical cell-site records. Between *Carpenter* and *Microsoft*, it's shaping up to be a really big Supreme Court term for digital evidence collection.

Justice Department moves to end routine gag orders on tech firms

The Washington Post

By Ellen Nakashima October 24

The Justice Department has issued new guidelines aimed at providing more transparency around prosecutors' secret demands for customer data stored on tech firms' servers.

The binding guidance, approved last week by Deputy Attorney General Rod J. Rosenstein, ends the routine imposition of gag orders barring companies from telling customers that their email or other records have been turned over in response to legal demands.

It also bans — in most cases — indefinite gag orders that forbid a company from ever telling users that their data has been searched.

Should companies be able to 'hack back'?

iapp Privacy Perspectives Amanda O'Keefe, CIPP/US

Current law makes that difficult.

The **Computer Fraud and Abuse Act** (CFAA) prohibits unauthorized access to a computer, without specifying intent or methodology. Enacted in 1986, the CFAA's applicability to current technology is unclear, creating a gray area for companies wishing to deploy cyberthreat defense mechanisms outside the perimeter of their own firewalls. A bipartisan bill formally introduced in Congress Oct. 13 aims to address that gray area by amending the CFAA.

Thank You

GTC

LAWYERS + STRATEGISTS