Changing Norms in Global Privacy: Emerging Issues & Law Firm Risks

Moderator:
Craig A. Newman, Patterson Belknap Webb & Tyler LLP

Panelists:
Austin Berglas, K2 Intelligence
Michael F. Buchanan, Patterson Belknap Webb & Tyler LLP
Stephan Menzemer, Graf von Westphalen
History of Law Firm Data Breaches

2008  •  Chinese hackers penetrate law firm network for more than one year and steal thousands of emails

2011  •  Law firm targeted by spear phishing emails that are linked to Chinese server

2012  •  “Anonymous” attacks, steals and publicly discloses 2.6 gigabytes of emails from firm that represented soldier who pled guilty in connection with killing of Iraqi civilians
       •  “Watering Hole” attack infects law firm website with malware transferred to visitors of web site

2015  •  Hackers infect law firm network with “ransomware” that encrypted firm files until ransom was paid

2016  •  Two major New York law firms acknowledge “data incidents”
       •  Panama Papers “leaked” (11.5 million documents) from Mossack Fonseca
       •  Edelson P.C. files federal class action under seal against “Chicago-based regional law firm”
          ▪  Motion to unseal is pending
          ▪  Fifteen additional class actions have been threatened
Agenda

• Today’s cyber threat environment: a clear and present danger for law firms
• A case study: Panama Papers & Mossack Fonseca
• Moving overseas: Microsoft v. United States
• E.U. Framework: an overview
• Ethics: a lawyer’s obligations
• Key takeaways
• Q&A
Law Firms Are Attractive Targets

- Hold sensitive, confidential client data
  - Mergers and acquisitions
  - Financial information
  - Trade secrets
  - Contract negotiations
  - PHI, PII and other protected information
- Aggregate valuable information from multiple sources in one place – improves hackers' ROI
- Law firms, as service providers, are targets of ransomware attacks
Threat Actors

- Hackers (hacktivists, nation-states)
- Terrorists
- Cybercriminals (ACH and credit card/ID fraud, ransomware attacks)
- Vendors (third parties, cloud provider(s))
- Competitors and Former Employees
- Insider Malfeasance/Misuse (employees, contractors)
- Human Error
How Organizations Learn About a Breach

How Compromises Are Being Detected
- 31% victims discovered the breach internally
- 69% victims notified by an external entity

Time from Earliest Evidence of Compromise to Discovery of Compromise
- 183 median number of days that threat groups were present on a victim's network before detection
- 24 days less than 2013
- Longest Presence: 2,982 days

Source: Mandiant 2016 Threat Report
Recent Headlines

June 21, 2016
“YORK HONOURS CANADIAN NAMED IN THE PANAMA PAPERS; U.S. SAYS HE WAS MIDDLE MAN IN COMPLEX CORRUPTION SCHEME”

April 7, 2016
“PANAMA PAPERS TIE MORE OF CHINA’S ELITE TO SECRET ACCOUNTS”

July 8, 2016
“PAKISTAN’S IMRAN KHAN SAYS PANAMA PAPERS SHOW PM'S INVOLVEMENT IN GRAFT”

September 7, 2016
“DENMARK TO BUY LEAKED PANAMA PAPERS IN TAX CRACKDOWN”

May 11, 2016
“PANAMA PAPERS’ FRESH LEAK REVEALS SINGAPORE NAMES”

May 22, 2016
“SCOTS LINKS UNEARTHED IN PANAMA PAPERS EXPOSE”

April 6, 2016
“PANAMA PAPERS: HUGE LEAK ALLEGES ELITES HIDING MONEY”

June 27, 2016
“PANAMA PAPERS SCANDAL: ‘THIS IS A REAL CRIME’”

May 9, 2016
“PANAMA PAPERS INCLUDE DOZENS OF AMERICANS TIED TO FINANCIAL FRAUDS”
What is Mossack Fonseca?

- A law firm based in Panama
- Founded in 1977
- Acts for about 300,000 companies
  - More than half are registered in British tax havens
More about Mossack Fonseca

- 600 staff in 42 countries
- Jersey, BVI, Isle of Man
Who are its clients?

- World leaders, oligarchs and despots, FIFA officials, the superrich, art dealers, crime bosses, and drug dealers
A laundry list of criminal activity

- Tax evasion
- Money laundering
- International arms dealing
- Bribery of public officials
- Terrorist funding
- Human trafficking
- Creating a black market for artwork stolen by the Nazis
What happened?

- Anonymous source provided 2.6 terabytes of data to German newspaper
- 11.5 million encrypted internal documents from 1970's through Spring 2016
  - Contracts, emails, correspondence, passport copies and certificates
- Hack or disgruntled employee?
How did the firm react?

- Started an investigation, supposedly secured its systems and notified its clients

Client Announcement

Important Information

April 1, 2016

Dear Clients:

This is to inform you that we are in the process of an in-depth investigation with experts who have now confirmed that unfortunately we have been subject to an unauthorized breach of our email server. If you have not heard from us until now, that means that we have reason to believe that your information was not compromised. We sincerely regret this event and have taken all necessary measures to prevent this from happening again.

At the moment, we are working with the help of outside consultants to determine the extent to which our system was accessed by unauthorized persons, what specific information those persons have obtained and the number of parties affected.

Below is additional information on this event and the actions we are taking. Rest assured that we accord the highest priority to the safety and confidentiality of your information. We employ multiple layers of electronic security and limit access to files to selected individuals within our firm in order to prevent breaches. As a result of this event, we have taken additional measures to further strengthen our systems.
What is the fallout?

- A global network of journalists created an interactive website, [https://panamapapers.icij.org/](https://panamapapers.icij.org/)
- They uploaded many of the records into a searchable database and published many articles identifying the clients, information about almost 320,000 offshore entities, and the officers, directors and beneficial owners of them.
More fallout

• Prosecutors around the globe have opened criminal investigations

• The Prime Minister of Iceland resigned

• Affiliates in the U.S. have closed their offices; Mossack Fonseca closed its offices in Gibraltar, Jersey and the Isle of Man

• Liquidated Mossack Fonseca Asset Management S.A., the financial services arm of the law firm
Moving Across the Pond:  *Microsoft v. United States*

- U.S. government warrant issued under Stored Communications Act sought email traffic that resided on a server in Dublin, Ireland
- The U.S. Court of Appeals for the Second Circuit held that email stored outside of the U.S. was beyond the reach of the SCA warrant
- Implications for Mutual Legal Assistance Treaties and cloud storage
- Next stop: Congress, rehearing *en banc* or U.S. Supreme Court
European Union’s legal data protection framework and its Implementation in Germany

• EU Charter of Fundamental Rights (Art. 8 Protection of personal data)
• Implementation of the Directive in all EU member states led to harmonization of European Data protection law
• Implementation of the Directive by the Federal German Data Protection Act (Bundesdatenschutzgesetz – BDSG)
• As of May 25, 2018 the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) will come into force. This regulation will be directly applicable in all EU member states (will not be discussed in detail).
European Union’s legal data protection framework and its Implementation in Germany (continued)

- German and European data protection legal framework applies only to “personal data”
  - “any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject).”

- “Personal data“ may be:
  - Client's name (or name of client's employees)
  - Client's email-address if client is identifiable
  - Bank data (e.g. International Bank Account Number (IBAN) und Bank Identifier Code (BIC))
  - Other data that enables identification of the client
Data transfer to a Third Country (e.g. USA)

**Two – Step Procedure**

Data transfers to a third country like the USA, require:

1. Admissibility of the data transfer itself
2. Adequate level of data protection
Data transfer to a Third Country (e.g. USA) - 2-Step procedure

1. Admissibility of the data transfer itself
   
   A. Consent of data subject or
   
   B. Permission by law

2. Adequate level of data protection
   
   ■ Does the third country in question ensure an adequate level of data protection (an adequate level will be assumed with regard to a transfer within the EU/ European Economic Region (EER), but not for the USA)?
   
   ■ If not, does a statutory exception apply?
Data transfer to a Third Country (e.g. USA) - 2-Step procedure (continued)

• What is an “adequate“ level of data protection?
  ■ Hard to (self-) evaluate for data controller / data exporter
  ■ EU-Commission's adequacy decision serves as a guideline
  ■ Based on a country’s domestic law or the international commitments it has entered into

• In case a country has not been found to ensure an adequate level, the most common standard tools to provide adequacy are:
  1. EU Standard Contractual Clauses
  2. Binding Corporate Rules
  3. EU-U.S. Privacy Shield (formerly Safe Harbor)
Statutory exceptions include:

• Consent of the data subject

• Transfer per se necessary for the performance of a contract which has been entered into or is to be entered into in the interest of the data subject between the controller and a third party (e.g. hotel room in Florida for German tourist)
Conflict area of US and EU interests and the possible invalidity of existing safeguards

- **EU interests:** Protection of EU citizen’s privacy rights
  - “I will not give you my personal data / the EU citizen’s data!”
- **US interests:** e.g. possible surveillance and access rights to prosecute criminal offences
  - “You have to hand over the data because we have authority to ask for it!”
EU-U.S. Privacy Shield

1. On July 12, 2016, the European Commission (Commission) adopted the EU-U.S. Privacy Shield

2. How does it work?
   - Companies are able to sign up to a Privacy Shield list with the U.S. Department of Commerce (DoC)
   - DoC verifies that companies’ policies comply with data protection standards required by the privacy shield
   - European companies may check whether their American partner companies, to whom they transfer personal data, are certified
   - 103 companies have been certified already, 190 are currently being checked, 250 are in the process of submitting their application (status: September 1, 2016)
3. The Commission decided that the EU-U.S. Privacy Shield ensured an adequate level of protection of personal data by reason of its domestic law and international commitments.

4. Věra Jourová, Commissioner for Justice, Consumers and Gender Equality: “It brings stronger data protection standards that are better enforced, safeguards on government access, and easier redress for individuals in case of complaints.”
EU-U.S. Privacy Shield (continued)

5. Critics and their concerns:

- Possibility for the U.S. government to perform bulk data collection in various cases
- Lack of independence of the ombudsperson, handling complaints or enquiries raised by EU individuals
  - EU-U.S. Privacy Shield does not fulfill the data protection criteria set up by the ECJ in the Safe Harbor decision and thus….
  - does not offer adequate protection for EU citizens against U.S. government authorities
2. Possible invalidity of existing safeguards

- On May 25, 2016, the Irish Data Protection Commissioner (Irish DPC) announced the intention to seek declaratory relief in the Irish High Court and a referral to the Court of Justice of the European Union (CJEU) to determine the legal status of data transfers under the EU Standard Contractual Clauses.

- In the eyes of the Irish DPC, the CJEU is bound to declare the EU contractual clauses invalid as it did with the Safe Harbor decision.

- Numerous professionals predict that the EU-U.S. Privacy Shield itself will eventually also end up in front of the CJEU.
  - development within this area should closely be observed
  - Which means can be considered a safe alternative?
...to be continued...
Privacy and Data Security: Ethical Rules Governing Lawyers

- Most states have adopted ethical rules closely following the ABA Model Rules
- Many state and local bar associations and committees have issued ethical guidance addressing data security
ABA Model Rule 1.1: Competence

- Lawyers must understand the risks associated with relevant technology, and must properly manage privacy and data security

- Standard Technology
  - E.g. email, document storage, document production software
    - See, e.g., Arizona Bar Op. 05-04, Alabama Ethics Opinion 2010-02

- Discretionary Technology
  - E.g. cloud technology
ABA Model Rule 1.6: Confidentiality

- Lawyer must “make reasonable efforts” to protect confidential data
- Internally (in the lawyer’s office)
  - Document storage; remote access to the firm’s server
    - See, e.g., NYSBA Op. 1019, Arizona 09-04
- Externally (vendors)
  - Evaluate vendors who manage cloud storage, payroll, or data services
ABA Model Rules 5.1 and 5.3: Supervision

- Lawyers must competently supervise subordinates and outside services who work with sensitive or confidential information, including PII and PHI
  - Associates, staff, outside vendors
  - Hand in hand with compliance under Rule 1.1
The “Reasonableness” Standard

- Implicit (Rule 1.1) and explicit (Rule 1.6)
- Neither fixed nor universal
- Must be addressed prospectively
  - See, e.g., NYSBA 842; Comment 16 to ABA Model Rule 1.6
- Some ethics opinions have attempted to define reasonableness, but context is key
  - See, e.g., NYSBA 1019, Pennsylvania Op. 2011-200
Professional Liability and Cybersecurity Insurance

- Review professional liability policy for cyber-related coverage
  - Cyber market is evolving and buyers have much flexibility
    - Consider appropriateness of “sub-limits”
  - Pricing has generally declined from peak in 2015
  - Consider scope of coverage including:
    - Crisis management costs
    - Business interruption costs
    - Recovery of vandalized data
    - Cyber extortion payments/ransomware
    - Wire transfer fraud
Key Takeaways & Questions
Austin P. Berglas is senior managing director and head of K2 Intelligence’s Cyber Defense practice. Drawing on his deep investigative experience in counterintelligence, national security, criminal cyber investigations, and incident response, Austin leads a team focused on advising global clients across all sectors on cybersecurity and cyber defense, providing proactive cyber defense, incident response, and threat detection in order to mitigate cyber risk, teaming with them to close gaps and proactively manage their assets.

Before joining K2 Intelligence, Austin served as assistant special agent in charge (ASAC) of the FBI’s Cyber Branch in the agency's New York office, where he oversaw all national security and criminal cyber investigations in the largest cyber branch in the FBI. Among the high-profile joint and international operations he managed were the dismantlement of the Blackshades organization and seizures of numerous TOR-based sites, including Silk Road and Silk Road 2.0. He led the criminal investigation into the computer network attack against JPMorgan Chase and established the Financial Cyber Crimes Task Force, the FBI’s first joint effort with the New York City Police Department (NYPD) and the Metropolitan Transportation Authority (MTA) to combat cyber threats and high-technology crimes affecting New York City and the nation.

Email: aberglas@k2intelligence.com  Phone: 917 243 7396
Michael F. Buchanan

Michael Buchanan is a litigation partner focusing his practice on white collar defense and investigations as well as patent litigation. He has tried several complex civil and criminal cases to verdict and argued multiple appeals. Mr. Buchanan regularly represents clients in cybersecurity law matters. Recently, he conducted an investigation on behalf of a financial services company regarding a potential data breach and provided counseling on breach notification and disclosure issues for the company. He co-authored an article analyzing the implications of the *In re Adobe Systems Inc.* data breach ruling for plaintiffs and has participated in the Practising Law Institute’s “Cybersecurity 2014: Managing the Risk” and The Law Firm Cyber Risk Conference, regarding data breaches, notification issues, and incident response strategies.

Before joining the firm, Mr. Buchanan spent over nine years at the U.S. Attorney’s Office for the District of New Jersey where he handled matters involving the Computer Fraud and Abuse Act, insider trading, the Foreign Corrupt Practices Act, health care kickbacks, off-label marketing, and Medicare/Medicaid and private insurance fraud. He received his J.D. from Brooklyn Law School and his B.S. from Columbia University.

Email: mfbuchanan@pbwt.com     Phone: 212.336.2350
Stephan Menzemer

Stephan Menzemer is a partner at Germany member firm GvW Graf von Westphalen, where he focuses his practice on information technology and telecommunications, contracts and national and international data protection. He is a commercial mediator, too. Stephan counsels leading IT suppliers and users and their management on all matters relating to their core business. He has provided advice in a number of significant German and international IT projects in the industrial, banking, public and IT sectors with the inclusion of near and offshore operations and outsourcing, public-private partnerships and public tenders as well as the establishment and verification of data protection and IT security structures.

Stephan is one of the most renowned IT-Lawyers in Germany. Since many years, he holds recommendations by major publications (leading IT-lawyer - Juve Handbuch Wirtschaftskanzleien, highly recommended lawyer - Legal 500, Germany's best Lawyer - Handelsblatt/Best Layers).

Stephan heads GvW’s IT/IP Practise Group. He has studied law at the University of Frankfurt/Main, the University of Aix en Provence, and the University of Marseille.

Email: s.menzemer@gvw.com  Phone: +49 69 800 85 19 86
Craig Newman is a recognized leader in both complex financial litigation and global cybersecurity. With more than twenty years as a litigation partner and General Counsel at both a multi-billion dollar international private equity firm and F500-owned media consortium, Craig represents Fortune 500 companies, their boards and leadership teams as well as investment funds, professional service firms, nonprofit organizations, manufacturers, technology companies and insurance companies.


He was recently named as one of the National Law Journal’s 2015 “Cybersecurity & Data Privacy Trailblazers.”

Email: cnewman@pbwt.com Phone: 212.336.2330