BRETTNER

CVITANOVIC

BCFIRM.LAW

Cyber 101

Presented by
Jacquline M. Brettner

NEW ORLEANS, LA
BCFIRM.LAW

About the Speaker: Jacquline M. Brettner

- Jackie is the Managing Partner of Brettner Cvitanovic. She practices in the areas of insurance coverage and commercial litigation, among others. Jackie is also a registered mediator and frequently assists businesses in resolving complex insurance coverage questions in order to minimize, or avoid, litigation costs.

- In her cyber practice, she assists corporate clients with in-house risk assessments. These evaluations focus on identifying cyber vulnerabilities, establishing protocols to minimize these risks, preparing tailored cyber attack and data breach response plans, and evaluating in-place risk management programs to ensure proper risk transfer. Jackie also facilitates cyber due diligence assessments for corporate clients evaluating prospective business partners and M&A targets.

- While she primarily represents corporate policyholders, Jackie also has experience counseling certain underwriters at Lloyd's of London, London market insurance companies, and domestic insurers.

So, What are we Talking About?

- A **cyber attack** can be broadly defined as a deliberate act through cyber space to manipulate, damage, or destroy computer systems or networks, industry control systems, personal computer devices, or other interconnected devices.
    - These attacks have the potential to create sweeping economic damage at a relatively low cost.
    - Recent examples also include efforts to deny access to computer networks or systems, and the encryption of valuable data held for ransom.
- A **data breach** is a security incident in which sensitive, protected, or confidential information is copied, transmitted, viewed, stolen, or used by an unauthorized individual.
    - Personally Identifiable Information (PII) is frequently targeted in a data breach. PII includes an individual's name, age, date and place of birth, social security number, telephone number, mailing and home addresses, biometric records, medical records, financial account information, among other identifying information.
    - Other targeted data include intellectual property, sensitive company information, client lists.
- Your odds of being struck by lightning this year at 1 in 960,000. Your odds of experiencing a data breach are 1 in 4.
- **Cyber liability policies** provide coverage for liabilities associated with cyber attacks, cyber security breaches, and violations of privacy and data breach notification laws.

The General Data Protection Regulation

- By its terms, the GDPR applies to the processing of personal data of "data subjects" who are in the E.U. by a "controller" not established in the E.U. (such as a U.S. domestic corporation) "where the processing activities are related to" either: (a) the offering of goods or services to such data subjects in the E.U. ***or*** (b) the monitoring of their behavior as far as their behavior takes place within the E.U.

- Thus, the purpose of the GDPR is to ensure that anyone in the EU is guaranteed adequate protection of their personal data globally by setting out broad and stringent rules about data collection and processing.
    - Like other privacy laws before it, the GDPR provides guidelines for the management of sensitive personal information by businesses.
    - It is the breadth of GDPR's pre-breach and post-breach obligations, its extra-territorial application, and the enormity of its potential penalties that set it apart.

GDPR's Accountability Principles

- Generally, Article 5 of the GDPR requires an organization ensure that personal data **shall** be:
  - Processed lawfully, fairly and in a transparent manner in relation to individuals;
  - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
  - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - Accurate and, where necessary, kept up to date;
  - Kept in a form which permits identification of data subjects for no longer than is necessary; and
  - Processed using appropriate technical or organizational measures in a manner that ensures appropriate security of the personal data.

- Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."
  - Purposely vague.

Critical Compliance Considerations

- **Extraterritoriality.**
  - The GDPR applies to organizations inside and outside the EU.
- **Broad Definitions.**
  - **Processing** means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means (e.g., collection, recording, storage, alteration, use, disclosure and structuring).
  - **Personal data** is also broadly defined as any information directly or indirectly relating to an identified or identifiable natural person, such as a name, identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
    - The U.S. has a much narrower definition by contrast.
  - **Data Subjects** are defined not just as individuals but can also include collections of data, such as an IP address and other data, that can later be associated with an individual.
- **Unfamiliar Terminology.**
  - A **data controller** is an organization that has control over and determines how and why to process data. A **data processor** is an organization that processes personal data on behalf of a data controller, typically a vendor or service provider.
  - Both have obligations under the GDPR, and data subjects can bring actions directly against either or both of those parties.
  - **Supervisory Authorities** or **Data Protection Authorities** (DAPs) are the various entities established within individual EU member countries and charged with the supervision of GDPR compliance.

Mechanics of Compliance: Follow the Data

- GDPR compliance means more than just updating an online privacy policy. Staging and scope of compliance recommendations vary depending on type of organization, data and data processes, EU footprint, and risk tolerance. Generally, however, the GDPR requires:
  - Map EU personal data processes;
  - accommodate the rights of EU data subjects;
  - implement accountability mechanisms;
  - mitigating risk in the supply chain; and
  - anticipate new data breach and cybersecurity obligations.

- Depending on the nature of violation, non-compliance fines under the GDPR include the greater of either:
  - €20m or 4 percent of global turnover, or
  - €10m or 2 percent of global turnover, depending on the nature of violation.

- Organizations must also continue to adhere to rules and EU-approved mechanisms regarding cross-border data transfers – typically ignored by U.S. Companies.

GDPR vs. Privacy Shield

- The burden on U.S.-based companies for documenting their privacy and data protection practices has increased substantially, compared to what it was under the Safe Harbor. **Thank you, Mr. Snowden.**
- The purpose of the GDPR is to ensure that EU residents are guaranteed adequate protection of their personal data globally by setting out broad and stringent rules about data collection and processing.
- By comparison, the Privacy Shield Framework was adopted as an new mechanism (along with the Binding Corporate Rules and the Standard Contractual Clauses) for legally transferring EU resident personal data from the EU to the U.S. This is just one aspect of the GDPR.
- Thus, while the Privacy Shield Framework does align with the GDPR to an extent, organizations that self-certified under the Privacy Shield are not GDPR compliant simply by virtue of their self-certification, and must take additional steps to document their compliance with the GDPR.

GDPR Specific Requirements/ Obligations

- To become GDPR compliant, Privacy Shield Certified entities will still need to meet a number of additional requirements, including:
- **Transparent Consent.** Freely given, for specific purpose, well informed, and easily withdrawn. For example, the GDPR make several impactful changes here by creating an "opt-in" threshold as opposed to "unsubscribe" requirement of the CAN-SPAM ACT of 2003, and adding the "coupling prohibition" and "function creep" requirements, among others.
- **Privacy by Design.** Certified entities must build privacy mechanisms and minimize processing as part of the design of their websites and practices.
    - Impacted Processes: website TOS/privacy policy, application TOS/privacy policy, design of lead capture forms, documentation of consent, re-permissions for existing database, "granularity" of use for services and permissions granted for specific smartphone/ browser usage on smart devices.
- **Data Protection Impact Assessments ("DPIA"):** Organizations will need to conduct assessments of their data collection and processing systems in addition to assessing the sufficiency of their security measures prior to processing data.
    - Factors considered: scoring/profiling, automatic decisions which lead to legal consequences, systematic monitoring, processing of special personal data, data which is processed in a large scale, the merging or combining of data which was gathered by various processes, data about incapacitated persons or those with limited ability to act, use of newer technologies or biometric procedures, data transfer to countries outside the EU/EEC and data processing which hinders those involved in exercising their rights.
    - Note: Blacklist and Whitelist processes w/in scope of EU representative or DPO. See, e.g., ISO/IEC 29134:2017 or Standard Data Protection Model.

GDPR Specific Requirements/ Obligations (cont.)

- **Record of Data Processing:** Obligation is imposed on the controller and their representative, but also directly on the processor and their representatives. Entities with less than 250 employees are arguably exempt; however, the caveats to the exception are unlikely to hold water.
  - Bottom line: Maintain records of all of your processing activities complete with index as this will be a go to favorite for auditors in the event of a breach and may eschew results where absent, similar to the effect of a negative evidentiary inference.
- **EU Based Representative:** Organizations with no physical presence in the EU that process EU resident data will need to appoint a representative within the EU for data subjects and DPAs to contact.
- **Record of Data Processing:** Organizations will need to maintain records of all their processing activities. right to file complaints with European Data Protection Authorities (DPA's).

GDPR Specific Requirements/ Obligations (cont.)

- The establishment of **Data Subject Rights** in their privacy policy and the ability to enforce the following data subject rights.
    - The right of access, restriction, and data portability.
    - The right to be forgotten, and to object to automated decision making and profiling.
    - The right to file complaints with European Data Protection Authorities (DPA's).

Preparing for Subject Access Request (SARs)	Complying with SARs
We can recognize an SAR and we understand when the right of access applies.	We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt.
We have a policy for how to record requests we receive verbally.	We are aware of the circumstances when we can extend the time limit to respond to a request.
We understand when we can refuse a request and are aware of the information we must provide when doing so.	We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.
We understand the nature of the supplementary information we need to provide in response to a subject access request.	We understand what we need to consider if a request includes information about others.

U.S Domestic Enforcement, you say?

- EU penalties under the GDPR are enforceable in the United States pursuant to state law.
- While many states have enacted the Uniform Foreign-Country Money Judgments Recognition Act, Louisiana has not. However, a Louisiana state court, pursuant to the rules of "comity" as articulated in *Hilton v Guyot,* 159 U.S. 113, 16 S. Ct. 139, 40 L.Ed. 95 (1895), would allow enforcement of the judgment from the court in the foreign country, provided the judgment creditor has the judgment recognized through an ordinary lawsuit. *See Baker & McKenzie Advokatbyra v. Thinkstream Inc.,* 2008-2535 (La. App. 1 Cir. 6/19/09), 20 So. 3d 1109, 1118.
- Thus, in Louisiana, an adjudicated penalty under the GDPR would be enforced domestically against the offending U.S. corporation if: (1) the rendering court had personal and subject matter jurisdiction; (2) the defendant had time and notice to present a defense; (3) there was no fraud involved in procuring the judgment; and (4) the foreign proceedings were according to civilized jurisprudence.
    - The first of these requirements being key and to be decided under "our" standards, i.e., *International Shoe's* "minimum contacts" test.

Better Late Than Never, no really.

- An April 2018 Ponemon Institute benchmark survey showed 40% of companies expected to achieve compliance only after May 25, 2018.
- This, despite the fact that 60% of business respondents recognized that the GDPR would "significantly change" their business workflows, and 71% acknowledged lack of compliance could hinder their business globally.
- Not unsurprisingly, the results showed that the high costs of compliance discouraged smaller businesses and/or those in unregulated industries with only one in five of those entities adding GDPR compliance costs as a budget line item – despite clear evidence of increasing technological reliance across the board.
    - The "low hanging fruit" approach of focusing on visible issues to regulators, such as, privacy policies, notices and consents, and subject rights, can be more costly in the long run.
    - While any move towards compliance is better than none, it would be unwise to put off the review/revision of less visible – but no less crucial – internal policies and procedures.

Key Takeaways

- Don't panic if you are not GDPR compliant – you are not alone.
- Continue to monitor developments.
- Take steps to address privacy and security aspects in your organization as follows:

Data Privacy	Data Security
Follow your data.	Undergo a benchmark data security audit.
Adopt privacy by design.	Continuously assess/manage security risks.
Describe and disclose practices.	Use encryption.
Handle sensitive data w/care + document your efforts.	Develop/enforce training and awareness.
Engage in de-identification.	Tailor data compilations to avoid unintentional discrimination.
Review/revise data retention practices.	Account for legal risks in developing profiles.
Review/revise consent processes.	Coordinate efforts between all relevant departments.
Re-evaluate vendor agreements + work together.	Review insurance placements and, in particular, cyber coverages.

Actions Taken

BRETTNER
CVITANOVIC
BCFIRM.LAW

NEW ORLEANS, LA

Lions, tigers, and Bears - Oh My!

- While exclusive jurisdiction over the interpretation of the GDPR rests with the European Court of Justice, a review of the various available DPA (Data Protection Authorities) opinions is instructive.
- Several different ways in which to slice their focus, i.e., industry driven, compliance aspects of regulation, geographic hotbeds, and/or major players.
- Hot Topics: Politics, Financials, Health Insurance, and Social Media…
- The UK's ICO issued the first formal enforcement action under GDPR in July 2018.
    - This action, a form of notice, required the firm cease processing any personal data of UK or EU citizens obtained from UK political organizations for certain enumerated purposes. See, e.g., Leave.EU & Eldon Insurance.
    - This investigation – characterized as the largest in history – continues to this day and is part of a larger regulatory effort to combat improper data retention/sharing in the political process.
- The Irish Data Protection Commission is fielding complaints from Privacy International against data brokers, credit-monitoring firms, and ad tech companies.

The Zoo Continued

- *Bupa Insurance Services, Ltd.* – an example of low hanging fruit approach gone wrong.
  - Employee exfiltration of half a million customer personal data.
  - Internal CRM Software.
  - Key phrases from decision are instructive.
    - A for Effort!

- Additionally, in the last several months of 2018, data protection authorities in Germany and France announced that they would start audits to check compliance with the GDPR.

  - Google was fined in January 2019 for € 50,000,000 due to its "lack of transparency, inadequate information, and lack of valid consent regarding ads personalization."

- Several other governments (such as Israel and Brazil) have moved on their own data privacy regulations to keep up with the GDPR regime.

Crystal Ball Predictions

BRETTNER
CVITANOVIC
BCFIRM.LAW

NEW ORLEANS, LA

Elementary, My Dear Watson.

- Although the U.S. wears the litigious reputational badge of (dis)honor, there are a variety of provisions within the GDPR that may encourage an increase in litigation and, perhaps even, class actions. These include:
  - The creation of individual rights of action including material damages and mental distress.
  - A reverse burden of proof requiring the accused organization prove compliance.
  - Expanded pockets = both data controllers & data processors can be separately held 100% liable for material damages if both were involved in the relevant data processing.
- Even greater imbalances between parties in the negotiation of vendor agreements w/potentially complex insurance coverage implications.
- Global push to recognize privacy as a "human right" or, alternatively, to drive the final nail in the coffin of our "right to privacy".
  - What will impact of Artificial Intelligence and Biometrics be?
- Simultaneously, the GDPR will (and already has) push other nation states towards a comprehensive framework.
  - China, Japan, Costa Rica, Panama, Brazil, the U.S., and yes, even Russia.

We're Number 2...Not Really

- The state of California passed the California Consumer Privacy Act in the summer of 2018, which provides GDPR-like protections and gives California consumers broader access and control over their personal information.
- The California law, which will take effect Jan. 1, 2020, will move the U.S. privacy regime in the direction of the generally applicable privacy laws that have applied extraterritorially for years.
- We anticipate that this trend will continue, with GDPR-inspired data protection soon becoming the new normal.
    - Recently, Utah became the first U.S. state to place into effect a comprehensive electronic data privacy law requiring warrants be obtained by police seeking discovery of certain electronic communications.
- Although a major focus of the world's attention is on the EU and U.S. compliance standards, many other countries have already implemented similar standards to the GDPR and had, indeed, done so before the GDPR's effective date. Among them: Russia, UAE, and the People's Republic of China.

All Things Cyber

BRETTNER

CVITANOVIC

BCFIRM.LAW

NEW ORLEANS, LA

Quantifying Data Breaches

- A 2017 Ponemon Institute study calculated the average total cost of a data breach incident to be $3.62 million. In 2018, that had risen to $3.86 million, a 6.4% increase.
- To put that in perspective, Target's 2013 data breach cost $252 million – before insurance and tax deductions. 3 billion accounts were affected, and this remains the largest corporate breach in history.
- While liabilities and costs can be driven by company size, businesses of all sizes and industries are vulnerable.
    - As of 2016, the average cost of a data breach for small businesses was $36,000. Up from $8,699 in 2012.
- Adding insult to injury:
    - Businesses that have experienced a "material" data breach are 27.7% more likely to experience another breach in the two years following the initial breach.
- Assessing cyber vulnerabilities, developing protocols to minimize risks, and reevaluating risk management programs to ensure proper risk transfer must be a top priority.

Just in the Last Two Years

- In 2017, Yahoo revised its estimate of the total user accounts compromised in its 2013 data breach from 1 billion to 3 billion.
- After 146 million accounts were hacked in 2017, Equifax CEO, Richard Smith, testified before Congress:
  - Dealing with 4 breaches, not 1.
  - Questions arise as to Equifax's delay in reporting the incidents, the reasonableness of its pre-incident security protocols, and whether or not the breaches actually provide the company with additional revenue streams.
- In 2018, the Securities and Exchange Commission fined Yahoo for its failure to disclose the 2014 hack affecting at least 500 million users, and Marriott/Starwood announced that the information of 500 million guests had been compromised.
- The number and size of breaches in recent years have led to increased focus on cyber law and data privacy.
- On the horizon:
  - Mandatory minimum monetary damages for compromised individuals.
  - Statutory fines and penalties for certain industries or "too big to fail" players.
  - Increased federal regulation, beyond HIPAA and GLBA.

Cyber Liability Policies

- Generally speaking, the coverages provided by cyber liability policies can be broken into "first-party" and "third-party:"

First Party Liability Coverage	Third-Party Liability Coverage
Forensic investigation of the breach	Legal defense
Legal advice to determine notification & regulatory obligations	Settlements, damages, & judgments related to the breach
Notification costs of communicating the breach	Liability to banks for re-issuing credit cards
Offering credit monitoring to customers	Costs of responding to regulatory inquiries
Public relations expenses	Regulatory fines and penalties
Loss of profits & extra expense during the time network is down	

1st Party Costs - Cyber Cinderella

- **Forensic Investigation Costs**
  - Investigation, identification, and isolation of breach.
  - Legal fees to pinpoint triggered notification and regulatory obligations.
- **Notification Costs**
  - Data and Industry driven.
  - 50-state patchwork, plus federal regulatory frameworks.
  - Varying notification requirements internationally – particularly in the EU
- **Business Expenses**
  - Lost profits or loss of customers following a breach.
  - Extra expenses associated with response:
    - PR fees;
    - Legal expenses generated by vendor and other third-party contract review to identify contractual notice, indemnity and/or other obligations triggered by breach; and
    - Credit monitoring expenses for any individuals affected, among others.

3rd Party Liability - The Shaggy Principle

- **We Don’t Buy/Sell Online**
- **My Business is Not a Target**
- **We Transfer Liability via IT Vendors**
- **We Have Ironclad Security Protocols**
- **Our CGL Covers It**

Stand Alone Cyber vs. Cyber Endorsements

- Some insurers offer cyber liability and data breach insurance coverage via endorsement to CGLs and/or Business Owner policies.
  - Cost-effective, entry level option for cyber risk transfer.
  - Typically, geared towards first-party costs with more limited coverages for third-party liabilities.

- Stand alone cyber liability policies offer completely different coverages:
  - Network & Privacy
  - Internet Media
  - Regulatory Proceedings & Fines
  - Payment Card Industry/Loss (PCI)

Cyber Liability in "The Cloud

- Transferring custody of data = does not transfer liability.
- Cloud based storage = does not eliminate cyber threats.
- Legal obligations rests with the company that initially accepts data.
- Customers may sue company who stored data with cloud provider, even though company itself was not responsible for data breach.
- Cloud provider recovery generally limited to contractual amount or multiple thereof.

Best Practices for In-House and Outside Counsel

BRETTNER CVITANOVIC

BCFIRM.LAW

NEW ORLEANS, LA

Company Responsibilities

- **Due diligence.** Take reasonable steps to assess your company's vulnerability to cyber attacks and potential liabilities associated with data breaches.
  - Data Type(s) & Volume
  - Software & Vendors
  - Industry(ies) & Market(s)
  - Technologies
- **Best Practices – Prevention.** Partner with a IT, HR, legal, and risk management professional to: (i) evaluate potential attack/breach scenarios, (ii) create protocols to eliminate/minimize risks and detail response procedures, and (iii) re-assess your risk management program to fill any gaps in coverage.
  - Security & IT patches
  - HR components
  - Risk transfer
- **Best Practices – Response.** Follow are previously implemented protocols. Work with your broker and counsel to shepherd you through the process.
  - Isolation
  - Preservation
  - Notification
  - PR
  - Insurance claim & adjustment

Best Practices for Cyber Placements

- What are the company's specific cyber risks? Professional evaluation.
- Are policy limits and sub-limits adequate for existing needs?
- Is there retroactive coverage for prior unknown breaches? Caution!
- Is there coverage for claims resulting from vendors' errors?
- Is "loss" of data covered or just data "theft"?
- What about first party property damage?

Best Practices for Cyber Placement (cont.)

- Can cyber insurance be combined with vendor indemnities to maximize protection? Caution!
- Does the policy cover data hosted by cloud providers? LOL issues!
- Will the insurer offer a subrogation waiver? Business Relationships!
- How does the cyber policy fit within the company's overall insurance program? Professional evaluation.
- Can more favorable provisions, limits and premiums be negotiated with another carrier? Traditionally driven by risk/company size.

Cyber Applications, Generally

- chief information officer or chief technology officer;
- history of security incidents and breaches;
- prior threats to company's network or website;
- facts or circumstances that reasonably could give rise to a claim under a prospective cyber policy;
- volume and types of data handled or maintained by the company;
- security standards and regulations, and frequency of assessments;
- existing network security programs, antivirus software, and intrusion testing;
- prior cancelation/refusal to renew a cyber policy;
- security budget;

Cyber Applications (cont.)

- audits of third-party service providers;
- vendor contracts and policies;
- practices concerning data encryption, passwords, patching and system access control;
- employee hiring and training practices, and procedures around termination;
- physical security controls (e.g., access cards);
- existence of written, attorney-approved and updated policies and procedures concerning the handling of information;
- policies governing mobile devices and social media; and
- data backup procedures.

Not All Policies are Created Equal

- Cyber policies are written as "claims made" or "claims made and reported" policies.
  - Retroactive date considerations are crucial where the affecting malware can lay dormant for years before an incident is detected.
  - Timely reporting even more important.
- There is now an ISO standard cyber liability policy form; however, still flexible coverages. What is impact of mandatory arbitration provisions?
- Like any insurance policy, the key to determining coverage is in the exclusions and the exceptions to the exclusions generated from endorsements.
  - Drawbacks and opportunities created by lack of uniformity.
  - Modular coverages and sub limits can present challenges if you are unfamiliar with varied policy forms.
- Looking to other policies to fill the gaps in – or take the place of – a cyber liability policy is much more difficult with cyber liabilities.
- Cyber claims to CGL and other policies have been tested, and mainly rejected, by the Courts.
  - ISO Data Loss Liability Exclusion
- Consider "buy-back" coverage with specialty endorsements and/or manuscripted policies.

Back to the GDPR: What Should You Look For?

- Cyber risk is not standardized, so you have to review your policies carefully. GDPR compliance will often be in the form of government fines or penalties. Are those covered by your insurance policy? Frequently not. What about costs respond to the cyber threat and restore your systems?
- Even if fines by regulators are covered, which regulators? Are international regulators included? This becomes increasingly important as data privacy laws take a more global approach.
- Most favorable venue provisions for penalties and fines—what does this mean for GDPR-cyber coverage going forward and how can you analyze your risk?

Questions? Comments? Let's Connect!

Jacqueline M. Brettner
brettner@bcfirm.law