Recent Developments in Guidance and Requirements for Breach Reporting

Mark Bauer, Professor of Law, Stetson University College of Law, Gulfport, FL

This roundtable will discuss recent developments in guidance regarding breach reporting, including issuances from Canada’s Privacy Commissioner on requirements, France’s Commission on Informatics and Liberty on GDPR and blockchain, and Ohio’s new privacy law with safe harbor.
RECENT DEVELOPMENTS IN GUIDANCE AND REQUIREMENTS FOR BREACH REPORTING

ABA Cyberspace Law Institute & Winter Working Meeting
January 25, 2019
Roundtable Discussion
Professor Mark D. Bauer
Stetson University College of Law
Discussion Leader
SURVEY OF RECENT DEVELOPMENTS

Bulgaria
Canada
France
Germany
Ireland
Serbia
United Kingdom
United States
BULGARIA

• Bulgaria adopted its national implementation of the GDPR on November 13, 2018.

• Bulgaria now requires government notification of a data breach within two hours of detection.
  • That notification may simply identify that a breach has occurred. Full notification must take place within GDPR standards.
Breach of Security Safeguards Regulations went into effect November 1, 2018. Rules were created under Digital Privacy Act, an amendment to the Information Protection and Electronic Documents Act (PIPEDA).

Regulations require organizations to:

- Conduct a risk assessment regarding "real risk of serious harm" to individuals.
- Provide notice "as soon as feasible" -- no specific time limit.
- Maintain records of all security incidents for 24 months from the day organization learns of breach.
- Further, organizations must provide extensive notice and information to the Privacy Commissioner regarding the breach and steps taken to inform individuals and mitigate harm.
- Penalties are up to C$100,000 per offense, with each individual constituting a separate offense.
Notification to the Commissioner must be in writing, and must include (to the extent known):

- a description of the circumstances of the breach and the cause;
- when the breach occurred;
- a description of the affected personal information;
- the number of affected individuals;
- a description of the steps that the organization has taken to reduce the risk of harm to affected individuals or mitigate such harm;
- a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach; and
- the name and contact information of a person who can answer the Commissioner’s questions about the breach.

Notification to individuals may be made “in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances” and must include (to the extent known):

- a description of the circumstances of the breach;
- when the breach occurred;
- a description of the affected personal information;
- a description of the steps the organization has taken to reduce the risk of harm that could result;
- a description of the steps affected individuals could take to reduce the risk of harm or to mitigate such harm; and
- contact information that the affected individual can use to obtain further information about the breach.
EUROPEAN UNION

Extraterritorial Application of GDPR

• The EU released draft guidelines regarding extraterritorial application of the GDPR on November 18, 2018. These guidelines were not as extensive or comprehensive as many commentators had hoped. The guidelines covered controllers and processors when one is inside the EU and the other is not.
• The comment period ends January 18, 2019 and final guidelines will be published in April 2019.

Comment in U.S. Rulemaking Process:

• The EU submitted a comment to the U.S. Department of Commerce in response to the National Telecommunications and Information Administration's request for comments on consumer privacy.
• The EU noted that while there are many state breach laws, organizations and individuals would benefit from federal harmonization of these rules.
Is GDPR compatible with Blockchain?

National Commission for Informatics and Liberties (CNIL) released an initial analysis in September, 2018. CNIL notes that its authority in France includes all personal data, and includes personal data stored in blockchain.

The inherent tension between GDPR and Blockchain includes:

- The right to be forgotten v. the permanence of blockchain
- Privacy by design v. the rigidity of blockchain design
- Responsible persons, data processors, and data controllers v. the inherent decentralization of blockchain
• CNIL suggests that any potential use of blockchain consider whether privacy by design can be met prior to adopting blockchain. In other words – do you really need to use blockchain?

• CNIL states that in many cases, anyone registering data in blockchain is a data processor responsible person. Without other arrangements, all participants in a blockchain could be deemed data processors.
  • Public blockchains present novel and challenging issues under the GDPR.
  • Personal data should not be stored unencrypted in blockchain.
  • Is every data writer a data controller? Can there be a way to assign responsibility?
  • Can collusion attacks be avoided?
  • Is right of erasure technically impossible? Would permanent encryption work?

• CNIL calls for an all-European response to blockchain and whether it can conform to GDPR, particularly with regard to the right of erasure/right to be forgotten.
• Can a company notify authorities that a competitor has failed to comply with GDPR or had a data breach?
• Specifically, is a violation of the GDPR a form of unfair competition and unlawful under German law?
<table>
<thead>
<tr>
<th>Date</th>
<th>Court</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 Aug. 2018</td>
<td>Bochum Regional Court</td>
<td>Company website failed to comply with GDPR. Competitor alleged non-complying website violated GDPR and Germany’s prohibition against unfair competition. Court held GDPR does not grant a competitor standing.</td>
</tr>
<tr>
<td>13 Sep. 2018</td>
<td>Würzburg Regional Court</td>
<td>Lawyer complained that another lawyer’s website failed to comply with GDPR. Court held GDPR violation could also violate unfair competition law.</td>
</tr>
<tr>
<td>25 Oct. 2018</td>
<td>Federal High Court of Hamburg</td>
<td>Some violations of GDPR may impact competition and violate unfair competition law. Must be determined on a case-by-case basis.</td>
</tr>
</tbody>
</table>
On May 25, 2018, Ireland imposed specific regulations on breach reporting. Companies must declare a "risk rating" for the breach, considering the nature and cause of the breach, the type of data exposed, mitigating factors, and whether the breach involves the personal data of vulnerable individuals.

The classification categories are:

- **Low Risk**: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal
- **Medium Risk**: The breach may have an impact on individuals, but the impact is unlikely to be substantial
- **High Risk**: The breach may have a considerable impact on affected individuals
- **Severe Risk**: The breach may have a critical, extensive or dangerous impact on affected individuals.
NEW IRELAND RULES

- All breach notification forms must be emailed to: breaches@dataprotection.ie
- All national breach notifications must be notified using the National Breach Notification Form.
- All cross-border personal data breaches must be notified using the Cross Border Notification Form.
- Telecom/ISP breaches must be reported on a specific form.
- The subject line of the email informing the Data Protection Commission must indicate whether the notification is new or an update, the organization's name, and a self-declared risk rating.
In November Serbia passed the Personal Data Protection Law, which becomes effective August 21, 2019. The new law is closely modeled on the GDPR.

Like the GDPR, data breaches must be reported within 72 hours, and individuals must be notified if the breach is likely to result in a high risk to the rights and freedoms of individuals.

Data processors must also notify the relevant data controllers in the event of a breach.

Penalties are substantially lower than the GDPR: €17,000 maximum.
Regarding Brexit, the draft withdrawal agreement released in November 2018 states:

• The GDPR will apply to personal data of EU citizens stored in the UK until at least the end of 2020.

• It is the intent of the parties that the UK will provide a level of security equivalent to that of the GDPR beyond 2020.

• After March 2019, entities will not be permitted to designate the UK Information Commissioner as lead authority for GDPR purposes.
New Ohio data breach law creates safe harbor for businesses meeting specific cybersecurity standards.

Safe harbor applies only to tort claims (not contract) based on Ohio law or brought in an Ohio court.

Law provides an affirmative defense; it does not bar suits

Law in effect November 2, 2018.
NEW OHIO RULES

• Companies must reasonably conform to:
  • The NIST Cybersecurity Framework, NIST’s SP 800-171, SP 800-53, or SP 800-53a, FedRAMP, the CIS Critical Security Controls, or the ISO 27000 family;
  • For regulated entities, the cybersecurity requirements of HIPAA, the Gramm-Leach-Bliley Act, FISMA, or HITECH, as appropriate; or
  • The PCI Data Security Standard (PCI DSS) in conjunction with one of the other standards listed in (1) or (2).
• Companies regulated by sector-specific laws may use conformity as an affirmative defense (e.g. following requirements of HIPAA).
• Alabama (eff. June 1, 2018): SB 318 requires companies with data breaches to notify impacted state residents within 45 days of notice/discovery of breach.

• Arizona (eff. April 11, 2018): HB 2154 amends Arizona’s data breach law to require notice within 45 days.

• Colorado (eff. Sept. 1, 2018): HB 1128 requires covered entities to provide notice of data breaches affecting more than 500 Colorado residents.

• Connecticut (eff. October 1, 2018): Individuals impacted by a breach including Social Security numbers are entitled to 24 months of credit monitoring. A previous law required 12 months of monitoring.

• Louisiana (eff. August 1, 2018): Act 382 requires affected Louisiana residents to be notified of a data breach within 60 days.

• Oregon (eff. June 2, 2018): SB 1551 requires Oregon residents to be notified within 45 days of data breach.

• South Carolina (eff. Jan. 1, 2019): H4655 requires that insurance companies must notify the Insurance Commissioner of data breach within 72 hours.

• South Dakota (eff. July 1, 2018): SB 72 requires affected individuals to be notified within 60 days of data breach.

• Vermont (eff. January 1, 2019): H 764 requires data brokers to register with Vermont Attorney General and make annual reports regarding security practices and breaches.

• Virginia (eff. July 1, 2018): HB 183 requires income tax preparers (including individuals) to notify the Virginia Department of Taxation of data breaches.
UNITED STATES – RECENT CASES

• Hutton v. National Board of Examiners in Optometry
  • 892 F.3d 613 (4th Cir. 2018)
  • A group of optometrists were victims of Identity Theft and had multiple Chase credit cards opened in their name. They found each other through a Facebook optometrist discussion group and determined that the only commonality between them was that their personal data was stored by the National Optometry Board.
  • The optometrists accused the Board of data breach. One month later the Board denied the breach; a few days later the Board said it would investigate further. The Board never denied or acknowledged responsibility.
  • The trial court dismissed because of insufficient injury (plaintiffs were not forced to pay fraudulent credit accounts) and because plaintiffs failed to sufficiently allege that any injuries were traceable to the Board.
  • Court of Appeals reversed and held for plaintiffs. 1) The fraudulent accounts and potential for future identity theft was sufficient injury. 2) The complaint's allegations regarding the Board were sufficient to survive dismissal.
Dittman v. University of Pittsburgh Medical Center


Employees of medical center sued employer for negligence and breach of implied contract after a data breach released personal information.

Trial court held that there was no duty of care if loss was solely economic. Trial court further held that data breaches are "widespread and frequent" and lawsuits would overwhelm the court system. The court further opined that there are no generally accepted standards for reasonable care of data. An intermediary appellate court affirmed.

The PA Supreme Court reversed. An employer has a common law duty to protect employees from unreasonable risk of harm. The fact that there may be a criminal component and that the employer may also be a victim does not preclude private civil recovery.

The Court also held that PA's economic loss doctrine does not preclude all negligence claims seeking only economic damages if the duty arises independently of contract.
MARK D. BAUER

Professor of Law
Stetson University College of Law
1401 61st St. South
Gulfport, FL  33707
mbauer@law.stetson.edu
727-562-7861