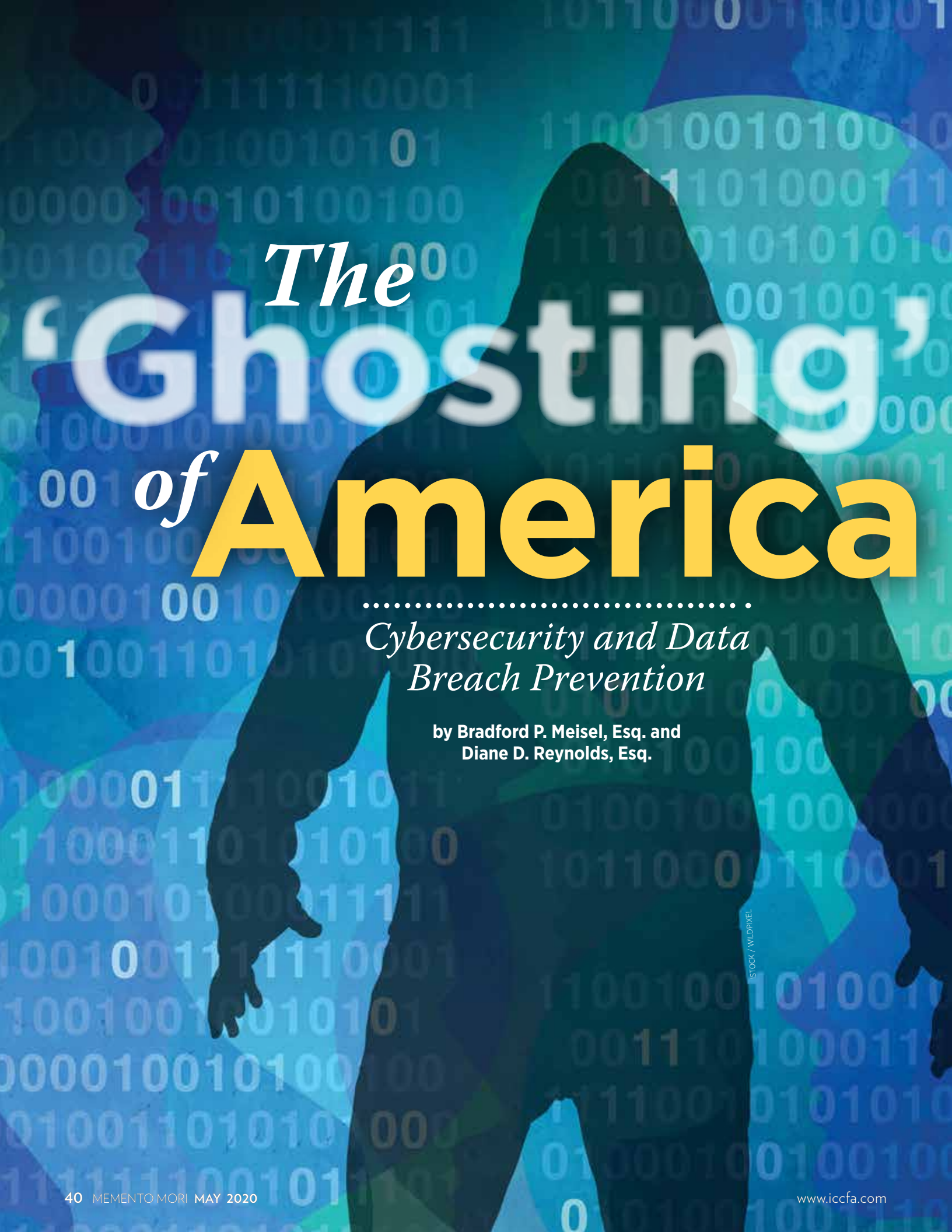

The 'Ghosting' of America

Cybersecurity and Data Breach Prevention

by Bradford P. Meisel, Esq. and Diane D. Reynolds, Esq.

ISTOCK / WILDPIXEL

ON OCTOBER 20, 2017, hackers successfully infiltrated the internet servers of Louisiana's Griffin Funeral Home in the middle of the night (as reported on Myarklamiss.com, Oct. 20, 2017). Employees found themselves unable to access the funeral home's email servers. The hackers also sent out emails purportedly from the funeral home's co-founder claiming she was stranded overseas and begging recipients to wire her money.

This cyberattack was just one of countless data breaches suffered by businesses across countless industries in recent years. According to a 2019 report by cybersecurity firm 4iQ, data breach incidents increased by 424 percent between 2017 and 2018 and small businesses have become leading targets for hackers seeking personal data for large-scale identity theft schemes.

In recent years, hackers have begun to target the personal information of recently deceased individuals in a process popularly known as "Ghosting." According to the American Association of Retired Persons, identity thieves used the identities of more than 700,000 deceased Americans to "open credit card accounts" or obtain services.

And since it can take up to six months for the Social Security Administration, financial institutions, and credit reporting agencies to process death records, while grieving family members are unlikely to check their recently deceased loved ones' credit, such Ghosting activity often goes undetected for weeks or months.

In 2018, *The Independent* reported that cybersecurity researchers observed hackers selling large collections of recently deceased patients' medical records containing names, Social Security numbers, phone numbers, addresses, dates of birth, and insurance information on the dark web.

Since funeral homes, cemeteries, and crematoriums possess such information about decedents that can be used to steal their identities but are not subject to the stringent data security laws and regulations governing health care, these businesses are appealing targets for hackers seeking to assemble collections of personal information for use in large-scale Ghosting schemes.

Shortcomings of the Funeral Rule

Funeral homes, cemeteries, and crematoriums are not subject to comprehensive federal privacy laws, and the Federal Trade Commission's Funeral Rule governing the funeral industry does not address data security or confidentiality. As a result, funeral homes, cemeteries, and crematoriums can potentially face serious legal consequences as a result of data breaches.

Only four states impose privacy obligations on funeral service providers enforceable by state licensing or oversight boards:

- Georgia requires funeral directors to safeguard decedents' confidentiality, privacy, and dignity.
- Ohio prohibits funeral directors and crematory operators from disclosing the "confidences, privacies, confidential facts, confidential opinions, or secrets of life of any person."
- Washington prohibits funeral directors from disclosing "information as to illness, cause of death, financial affairs, or transactions, and any other information customarily considered confidential."
- Virginia prohibits funeral service providers from disclosing information regarding infectious diseases harbored by decedents.

While it is currently unclear whether the disclosure of confidential information as a result of a data breach would violate these laws, funeral service providers could potentially face discipline in Georgia, Ohio, Washington, and Virginia under such circumstances.

Broader Legislative Action

Numerous states have enacted data security and privacy statutes that could apply to funeral homes, cemeteries, and crematoriums. States including New York, Florida, Massachusetts, and Texas, have enacted statutes requiring entities that own or license personal information to implement and maintain reasonable security procedures appropriate to the nature of the information and the size and operations of the entity, which are enforceable by state Attorneys General or administrative agencies.

The CCPA

The California Consumer Privacy Act (CCPA), which took effect on January 1, 2020, requires any business that fits the following criteria to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information: (A) "does business in California"; and (B) has annual gross revenues over $25 million; (C) alone or in combination buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices; or (D) derives 50 percent or more of its annual revenues from selling consumers' personal information.

Larger funeral homes, cemeteries, and crematoriums, including those outside California that service California decedents or handle funerals paid for by California residents, could be subject to CCPA, which entitles data subjects to bring private actions for violations of the duty to implement and maintain reasonable security procedures for the greater of "actual damages" or $100–$750 per customer per incident.

The GDPR

The European Union General Data Protection Regulation (GDPR) took effect on May 25, 2018, and imposes stringent requirements on entities that process the personal data of European Union (EU) residents in connection with offering goods or services to EU residents.

Therefore, funeral homes, cemeteries, and crematoriums in the EU, and those outside the EU that provide services to decedents who die in the EU or provide services paid for by family members residing in the EU, could be subject to GDPR.

> [F]uneral homes, cemeteries, and crematoriums in the EU, and those outside the EU that provide services to decedents who die in the EU ... could be subject to GDPR.

GDPR requires covered entities to document compliance, including creating a "record of processing activities" demonstrating they have secured an adequate legal basis for processing activities and made required disclosures to EU data subjects.

Funeral homes also handle "special categories of data," such as health-related information or information about individuals' religion, ethnicity, or preferences, which are subject to more GDPR stringent regulations. Moreover, covered entities must implement appropriate technical and organizational measures to protect the security of the personal data they possess and process.

Data controllers subject to GDPR must inform the relevant EU supervisory authorities within 72 hours of data breaches affecting personal data and are likely to adversely impact affected data subjects. Covered businesses outside the EU must appoint an agent-for-the-service-of-process type in an EU country to maintain compliance documents. Violations of GDPR are subject to a private right of action and administrative fines totaling up to 4 percent of an entity's annual global revenue.

Other State Action

Moreover, all 50 states and the District of Columbia have enacted statutes requiring any entity that owns or licenses their residents' personally identifiable information to inform all affected individuals of a data breach, often within specified timeframes ranging from 72 hours under California's statute to 90 days under Connecticut's statute.

Twenty-two such statutes, including those in California, Illinois, Massachusetts, New Jersey, North

Carolina, and Texas, provide a private right of action for violations while the other 29 statutes are enforceable by state Attorneys General or administrative agencies.

Therefore, in the event of a data breach, funeral homes, cemeteries, and crematoriums could be subject to numerous data breach notification laws.

A Higher Likelihood of Litigation

Given that the death and funeral of a loved one is often the most traumatic and emotionally charged event in a person's life, the funeral, cemetery, and crematorium industry may have greater exposure to claims than most other industries under data security and data breach notification laws.

Since a data breach related to the death and funeral of a loved one is likely to elicit a strong emotional response, especially one in which a hacker uses a recently deceased loved one's identity to create financial accounts and make purchases, those affected by a funeral home data breach may be far more likely to file lawsuits or reports with administrative or law enforcement agencies than those impacted by data breaches related to less traumatic and emotionally charged life events—such as retail purchases or vacations.

Moreover, individuals who suffer emotional distress as a result of a data breach of a recently deceased loved one may be able to recover substantial emotional harm damages from a funeral home, cemetery, or crematorium found to have violated data security or data breach notification laws.

The Long-Term Partnership Solution

Funeral homes, cemeteries, and crematoriums might consider partnering with an interdisciplinary team that retains and supervises appropriate technology professionals in order to evaluate their cybersecurity risk, develop, and institute measures to prevent data breaches, and ensure compliance with data security and breach notification laws.

Such an interdisciplinary team can develop and implement practical incident prevention and compliance strategies that fit the specific needs, budgets, and risks faced by each business. Such strategies may include:

- Determining how to best allocate financial resources for cybersecurity upgrades to software and hardware;
- Diligently vetting and selecting secure devices and software;
- Developing employee monitoring protocols; and
- Documenting and demonstrating compliance with data security requirements imposed by state, federal, and international law.

After the assessment is completed and the risks identified, deathcare professionals might consider purchasing cybersecurity insurance to cover liability in the event of a data breach, as well as business interruption and remediation costs incurred as a result of such an incident.

An interdisciplinary team headed by a law firm is the ideal partner for small businesses seeking to assess and upgrade their cybersecurity, since it:

- Allows for a reduction in overall costs by sharing the expertise of an established team of experts;
- Cloaks the process in attorney-client privilege that can limit discovery in the event of a lawsuit, administrative proceeding, or investigation; and
- Allows for one-stop shopping in which businesses can have the benefit of a single team capable of providing technical services and advice as well as legal advice regarding compliance, the legal implications of employee monitoring, and navigating the legal and public relations impact of cybersecurity incidents. ◼

Diane D. Reynolds, Esq., DReynolds@mdmc-law.com, is a partner at McElroy, Deutsch, Mulvaney & Carpenter, heading the Cybersecurity, Data Protection, and Privacy practice and has an extensive background in the representation of private and publicly held entities in mergers and acquisitions, corporate finance, compliance, corporate governance, and strategic growth initiatives. She possesses a unique depth of experience in privacy/data security combined with strong technology experience.

Bradford P. Meisel, Esq. BMeisel@mdmc-law.com, is an associate at McElroy, Deutsch, Mulvaney & Carpenter specializing in corporate transactions, cybersecurity, and data privacy, and previously served as a Senate Judiciary Committee Law Fellow to U.S. Senator Sheldon Whitehouse (D-RI) and Cybersecurity and Technology law clerk to U.S. Senator Gary Peters (D-MI).

Emotional Harm Damages: The Impact and Likelihood

As mentioned in a California appellate case, *Lieberman v. KCOP Television, Inc.*, other statutes entitling plaintiffs to "actual damages" entitle them to emotional harm damages, even though California courts have yet to determine the availability of emotional harm damages for CCPA violations.

According to case law, of the 22 states that permit private actions for violation of data breach notification statutes, four, namely **Illinois**, **Massachusetts**, **North Carolina**, and **Texas**, allow plaintiffs to recover emotional harm damages; three other states, however, namely **Maryland**, **New Jersey**, **Oregon**, and the **District of Columbia** prohibit plaintiffs from recovering emotional harm damages.

Given that courts in the other 14 states have yet to address the availability of emotional harm damages in such actions, it is possible that emotional harm damages could be available for violations of data breach notification requirements in up to 18 states.