Preface

This Supplement is current through January 2016.

The law surrounding cybersecurity and privacy has been rapidly changing. In fact, few areas of the law have seen the type of rapid change experienced in development relating to cybersecurity. This changing landscape has surrounded the writing and publication of this work. Many of these changes were occurring as the First Edition was being written and going to print. It is not surprising therefore that following publication of the First Edition, events relating to cybersecurity have continued to develop at a rapid pace. These recent developments have included efforts to develop a legal framework for dealing with cybersecurity and privacy, as well as efforts to make personal data and information more secure against a variety of threats.

A number of key developments have taken center stage. First, Congress finally passed legislation dealing with sharing of information relating to cybersecurity, over objections from privacy advocates.[1] The new legislation is intended to promote aggressive actions to combat cyber thefts and intrusions at an early stage, and for industry to work collaboratively together, and with governmental forces, to develop strong cybersecurity measures.[2] Whether that goal will be achieved remains to be seen. It is also an open question whether those critical of the measure based on the perceived adverse impact on privacy will unfortunately have been proven correct in their fears.

Second, the ability of the Federal Trade Commission (FTC) to deal with cybersecurity was firmly established in the case involving Wyndham hotels.[3] As the First Edition was going to print, the Third Circuit affirmed the district court judgment in that case, upholding the ability of the FTC to aggressively use the FTC Act to deal with lax cybersecurity controls.[4]

---

[1] *See* Cybersecurity Act of 2015, discussed in Supplement, Chapter 4, Section XVII.

[2] *See id.* Section XVII.C.

[3] *See* Federal Trade Comm'n v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 610–11 (D.N.J. 2014), *aff'd*, No. 14-3514, 2015 U.S. App. LEXIS 14839 (3d Cir. Aug. 24, 2015), discussed in Main Volume, Chapter 4, Section II.

[4] See Main Volume, Chapter 4, Section II.

Following the publication of the First Edition, the FTC and Wyndham settled the case, precluding any further review in that case of the FTC's ability to proceed in this area under the FTC Act.[5]

Third, guidance from federal agencies has continued to emphasize the importance of internal controls.[6] More specifically, various governmental agencies and offices emphasized the importance of training, education and expertise in dealing with cybersecurity matters.[7] A number of agencies have emphasized the importance of training and expertise even at the board level.[8] Congress is also considering legislation that would require disclosure of information relating to board expertise.[9] This inescapable trend strongly confirms the need for private enterprise to invest in the expertise and infrastructure needed to guard against personal data or information being lost or stolen. Courts will no doubt further encourage such investment by issuing rulings establishing liability for failing to take such precautions.

The First Edition described how advances in technology, coupled with the desire of some in society to derive illegal profits from technology advances, contributed to new challenges for Congress and the courts. These challenges have been made all the more difficult by the threat of terrorism, which has prompted law enforcement to utilize more aggressive tactics in order to uncover and eradicate terrorist forces. Congress responded to judicial challenges to the use of bulk data collection by passing legislation designed to strike a balance between the nation's security interests and the rights of individuals to maintain their privacy. This legislation, the USA FREEDOM Act of 2015,[10] likely will not end this debate. Law enforcement will no doubt continue to press for more aggressive data gathering unless and until the terror threat subsides. As there is no end in sight as to the terror threat, courts will be called upon in the future to fine tune that balance in the course of interpreting the provisions of this new legislation.

This Supplement has continued the approach taken in the First Edition. Namely, this Supplement includes an update of federal and state laws governing cybersecurity discussed in the First Edition.[11] Once again, it is important to stress that each of the statutes discussed in this Treatise could well deserve a chapter of their own, and once again, it should be

---

[5]*Id.*

[6]See Main Volume, Chapter 8, Section II.

[7]See Main Volume, Chapter 8, Section V.A.3.

[8]See Main Volume, Chapter 8, Section II. *See, e.g.*, FDIC, Security Standards for Customer Information, FIL-22-2001 (Mar. 14, 2001), *available at* www.fdic.gov/news/news/financial/2001/fil0122.html 9 (mandating board oversight).

[9]*See* S.2410, The Cybersecurity Disclosure Act of 2015, (114th Cong. 1st Sess. (2015-2016), discussed in Supplement, Chapter 8, Section II and contained in Appendix 3.C.

[10]"Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (the "USA FREEDOM Act"), P.L. 114-23 (June 2, 2015), discussed in Supplement, Chapter 4, Section X.

[11]See Main Volume, Chapters 2–4.

stressed that space and time limitations make it impossible to offer more of an in-depth treatment, and that the reader is cautioned that many legal issues are continuing to emerge, and fresh research will undoubtedly be necessary to address such issues. Similarly, as with the First Edition, this Supplement continues to deal separately with developments in two industries which deserve special treatment: the financial services and health care industries. This Supplement also follows the approach in the First Edition of trying to educate users of computer systems how they can protect themselves from lawsuits. As with the First Edition, a great deal of information can be found in materials generated by governmental agencies which have devoted substantial resources to educating industry about how it can protect itself, and in doing so, protect its customers and consumers from data breaches and unwarranted intrusions into computer systems. Once again, the reader may find it useful to consider some of these materials as "best practices," and others as worthwhile commentary on cybersecurity. For those facing governmental oversight or enforcement actions, awareness of governmental guidance is essential in rebutting claims that cybersecurity practices were lax or deficient.

Finally, this Supplement includes developments in litigation tactics and strategy. Just as the law in this area was developing when the First Edition was published, many of the legal precepts surrounding cybersecurity have continued to take shape during the writing and publication of this Supplement.

Finally, the same word of caution given in the First Edition is repeated herein: "treatises of this sort are intended to provide lawyers and clients alike with helpful information needed to address particular problems. But like many areas of law, the ultimate resolution will depend on unique facts, and legal developments. For that reason, this Treatise—while hopefully of substantial value to both lawyers and their clients—cannot replace the need for clients to consult with counsel about specific legal issues, and to address their own complicated factual and legal issues."[12]

March 2016

[12]See Main Volume, Preface.