PREFACE

This First Edition is current through June 2015, with significant additional developments through August 2015.

The information age saw three major shifts in both personal and business habits. First came the Internet, and with it the ability to obtain information on almost any subject. Those in the habit of walking outside to pick up their morning paper soon learned that they could, with the push of the "on" button, have access to the news from around the world, as well as the equivalent of the contents of most major libraries. This phenomenon soon morphed into "online" business and commercial dealings, as individuals learned that they could shop, and conduct a multitude of transactions online. Banking online became the new way of making deposits, cash transfers and many other transactions that would otherwise have required a trip to the bank. The same was true of health care. While there was no substitute for a trip to the doctor or hospital, patients were soon able to make appointments, view their charts online, and communicate with their doctors while sitting at home on the living room couch. The final major breakthrough was social media. Teenagers taught their parents that they were able to communicate, share photos and media, and keep "in touch" while sitting at their computers. This marvel led to a number of almost instant mega-companies capable of allowing millions of users to network for either business or social purposes.

It is an unfortunate testament to humankind that almost as soon as the internet, or "information age" began, individuals who had been intent on injecting viruses into computer programs began focusing their attention on the internet. Those who had "enjoyed" the challenge of planting viruses through infected computer programs saw even greater opportunities as mass marketing and other internet based activities opened up new horizons. While the computing public was in awe at the potential from this vast new store of information that was bringing with it advances in, among other things, education, science, and culture, the public was also in fear of the devastating impact on their computer systems from viruses, malware, and other material developed and disseminated to the unsuspecting public.

As a result of these events, an industry emerged which was designed to combat malicious computer programs and which had all it could do to keep pace with new and ingenious engines of destruction. New software and hardware was developed with one of two goals in mind: either to steal and sell the confidential or sensitive data of customers, consumers, businesses or governmental units, or alternatively, to wreak havoc on the public which was growing increasingly dependent on the internet and computers for home, business and even governmental use. Given this phenomenon of exponential growth in information systems, coupled with equally impressive efforts to illegally profit from those same systems, it should come as no surprise that legislators, lawyers, and judges have risen to the occasion, and have quickly stepped in to write new rules to address new problems caused by the information age phenomenon. The result is that the unparalleled growth of the internet is matched only by the unparalleled explosion of statutes, regulations, rules, judicial opinions and commentaries dealing with cybersecurity.

The response to this explosion of legal precedent has been remarkable. For one thing, an entire new legal sub-specialty was developed almost overnight. Many lawyers were drawn into this area by virtue of a background in intellectual property. Some have approached it with a

policy background, looking to assist legislators, lobbyists, and industry groups formulate laws, regulations, and policies that would either outlaw certain problems or conduct, or alternatively, prevent the natural growth of products and the industry. There was also a cadre of lawyers who were hired by large corporations to assist in data privacy and security. And yet other lawyers have approached the problem from the vantage point of litigation, and its impact on the internet and computer industry. This last approach is at the heart of this Treatise, which is designed to assist lawyers and clients in avoiding litigation by taking certain precautions, or if they cannot avoid litigation, responding to lawsuits in the most effective way.

This treatise therefore approaches the problem of cybersecurity from a number of different vantage points. First, it is impossible to either avoid litigation or deal with it effectively without having an understanding of the legal landscape. Accordingly, the first several chapters are designed to provide a summary of the statutory schemes that govern this new and emerging area of law. This survey of federal and state laws governing cybersecurity is offered with a frank admission that each of the statutes discussed in this Treatise could well deserve a chapter of their own. Due to space and time limitations, such an in-depth treatment is impossible, and the reader is cautioned that many legal issues are continuing to emerge, and fresh research will undoubtedly be necessary to address such issues.

While the intent was therefore to provide a survey of existing laws, there were two industries which deserve special treatment, and which are therefore dealt with separately. These areas include the financial services and health care industries. Because of the sensitive nature of the data or information handled in these two industries, legislators have developed a sophisticated set of laws, rules and regulations to deal with handling of such data or information in each of these two areas. The Treatise is intended both to address the legal requirements imposed on entities doing business in the financial services sector and health care industry, but also to give the reader a view to judicial attitudes towards existing laws, rules and regulations.

The next goal of the Treatise is to educate users of computer systems how they can protect themselves from lawsuits. Much of these materials are drawn from 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. The reasons for paying special attention to these materials is twofold: First, the best defense against litigation is to avoid it entirely by having in place secure and appropriate systems to guard against data breaches or intrusions. Because the materials provided by various agencies offer a sound game plan for doing so, readers are urged to consider some of these materials as "best practices," and others as worthwhile commentary on cybersecurity. Second, because governmental entities may confront the readers of this Treatise who suffer a data breach, it is helpful to understand exactly what requirements those, and other, governmental entities have recommended as precautionary tactics. The hope is that claims by the government of statutory violations, negligence, or malfeasance can be more adeptly addressed if readers are conversant with the government's own standards and advice for the computing public and businesses.

Finally, the third section of this Treatise is devoted to litigation tactics and strategy. As with the law in general, litigants learn from experiences of other litigants. The design of this third section is not only to offer a discussion of precedents and winning strategies, but to point the readers to decisions and precedents that will guide them in avoiding litigation, where possible. This discussion includes a review of precedents dealing with motions intended to address the most litigated issues governing access to the courts, namely, application of the pleading

standards articulated by the Supreme Court in *Bell Atlantic Corp. v. Twombly*[1] and *Ashcroft v. Iqbal*[2] standing requirements,[3] and where class actions are concerned, the demand futility requirements often relied upon to avoid shareholder derivative actions.[4] And because many of these cases are brought as class actions, which carry with them their own set of legal complexities, this Treatise addresses many of the legal issues surrounding the use of class actions in the cybersecurity context. As this discussion demonstrates, the development of certain of these legal precedents, particularly those relating to standing requirements, is still very much a "work in progress" in the courts, as shown by the Supreme Court's recent decision to grant a writ of certiorari in one case involving these standing requirements.[5]

Once inside the courthouse with a well-pleaded complaint, litigants must then address a number of issues relating to how to respond to the allegations in the complaint. Given the highly technical nature of these lawsuits, an almost unavoidable issue is the use of experts. Accordingly, this Treatise seeks to address a number of the most important issues, including qualifying experts, and making sure that those non-testifying experts retained to assist in the defense will not find themselves thrust onto the witness stand by virtue of a ruling that their work-product is somehow discoverable.

Another area of law which has consumed substantial attention is the propriety of damages arising from data breaches and cybersecurity issues. Creative litigants have devised a number of harms flowing from data breaches which have caused courts to address whether many of these claimed damages are simply too speculative to support a claim. While the legal principles surrounding these issues are not new, their application to data breaches and cybersecurity does raise interesting and novel questions for courts and litigants.

Finally, a word of caution, 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.

August 2015

Samuel Rosenthal

---

[1] 550 U.S. 544 (2007).

[2] 556 U.S. 662 (2009).

[3] *See* Chapter 12, Section V.

[4] *See* Chapter 11, Section IV.

[5] Robins v. Spokeo, Inc. 742 F.3d 409, 410 (9th Cir. 2014), *cert. granted,* Spokeo, Inc. v. Robins, 191 L. Ed. 2d 762 (U.S. 2015).