NOTES

FROM GIBBERISH TO JARGON: A LOOK AT THE TECHNICAL AND LEGAL ISSUES SURROUNDING NEW TECHNOLOGIES AND HOW THEY NECESSITATE ACTIVE ENGAGEMENT BY ATTORNEYS IN CLIENT DECISION-MAKING

*By Peter N. McClelland, CIPP/US**

INTRODUCTION 333
HYPOTHETICAL 334
DISCUSSION 336
I. CONTRACT DRAFTING ONLINE HAS UNIQUE CHALLENGES, AND TO CONFRONT THEM, ATTORNEYS MUST UNDERSTAND THE PLATFORM THEY ARE USING AND THE SPECIALIZED REQUIREMENTS THAT HAVE DEVELOPED AROUND THE UNIQUE NATURE OF A WEBPAGE. TO PROPERLY PROTECT CLIENT INTERESTS, LAWYERS MUST ACTIVELY ENGAGE IN THE LAYOUT AND FORMAT OF THE CONTRACT, NOT JUST ITS CONTENT 336
A. Specht v. Netscape provides a good framework from which attorneys can formulate contracts online because

* Peter McClelland received his Juris Doctor from Elon University School of Law in December 2017. He was a J.D. candidate at the time of authorship, and after authoring this piece he became a Certified Information Privacy Professional. He earned his Bachelors of Arts at the University of North Carolina at Chapel Hill in May 2015. He would like to thank his husband, Robert Kevan Schoonover McClelland, for his love and support. He would like to thank his parents, William and Ann Marie McClelland, for imbuing in him the love of learning that made this note possible. And he would like to thank Professor David Levine for his guidance in writing this note.

it provides clear requirements for assent based upon the technical abilities of webpages 337
B. Rather than settling for a browsewrap link to the website's terms of use, the attorney in our hypothetical should have insisted on a clickwrap agreement 339
II. CYBERSECURITY LAW IS GROWING RAPIDLY AND CONTINUES TO TOUCH A VARIETY OF ESTABLISHED LEGAL FIELDS, AND AS SUCH, ATTORNEYS MUST ASSUME A GREATER ROLE IN THE DECISIONS THAT CLIENTS MAKE REGARDING CYBERSECURITY ISSUES AND IN THE IMPLEMENTATION OF SUCH DECISIONS 342
A. First, a review of cybersecurity fundamentals is necessary for all attorneys who advise clients facing cyber threats or holding sensitive digital information 344
B. Next, a review of the law that has already cropped up around cybersecurity issues will reveal how the hypothetical attorney should have collaborated with the technology specialist on decisions regarding the governance and implementation of the cybersecurity program 349
CONCLUSION 363

INTRODUCTION

A lawyer is traditionally, though not exclusively, viewed as the advisor to his or her clients on legal matters.[1] Nearly every lawyer, law school, and client understands this traditional role. From the beginning of law school, on the bar examination, and through most of their practice, lawyers and aspiring lawyers almost intuitively understand their role in the traditional legal spheres. But ironically, cyber issues, which have interwoven themselves in nearly all of the traditional areas of legal practice, have often been pigeonholed as a "tech problem" for other industries' specialists to deal with.[2] This is particularly unfortunate, because "a lawyer's advice at its best often consists of recommending a course of action in the face of conflicting recommendations of experts."[3] This is to say that a lawyer is best when he or she is actively engaging in the client's decision-making process rather than deferring to other experts.[4]

In the following sections, this Note will argue that attorneys should be actively engaged and robustly participating—rather than deferential and resting on the expertise of other specialists—when clients make decisions regarding new technologies. To demonstrate that engaged and robust participation by an attorney is the preferable model for decision-making, this Note will begin by discussing a hypothetical situation in which an attorney is asked to work on a contract between the employing corporation and an online software company for a piece of cybersecurity software. It will then zero-in on the technical issues that emerge in the hypothetical situation, and discuss how these issues relate to the law surrounding new technologies. After identifying the technical and legal issues, this Note will then discuss how the hypothetical attorney could have better served his client through engaged and robust attorney participation in the client's decisions relating to that new technology.

---

[1] *See* MODEL RULES OF PROF'L CONDUCT r. 2.1 (AM. BAR ASS'N 2014).

[2] *See generally* Catherine J. Lanctot, *Becoming a Competent 21st Century Legal Ethics Professor: Everything You Always Wanted to Know About Technology (But Were Afraid to Ask)*, 2015 J. PROF. L. 75, 76–77 (discussing the nexus between technology and the legal profession).

[3] *See* MODEL RULES OF PROF'L CONDUCT r. 2.1 cmt. 4 (AM. BAR ASS'N 2014).

[4] *See generally* Alexander Scherr, *Lawyers and Decisions: A Model of Practical Judgment*, 47 VILL. L. REV. 161, 188–95, 269–74 (2002) (explaining that effective lawyering occurs by engaging the client and facilitating the decision-making process, rather than deferring to external experts).

HYPOTHETICAL

Envision an attorney who is employed at a mid-sized California company of middling sophistication, who primarily practices transactional and corporate law. He does not have a background in coding or computer science. He is asked to lead a team that includes a business specialist and a technology specialist. He will serve as the legal specialist and will negotiate a contract with an online software provider to acquire a cybersecurity program based upon blockchain for the team's employer.[5] The team is then tasked with setting up the policies and procedures that will govern the use and application of the software on their employer's webpage and over their corporate network. The software will come in two forms: the first would be commercial to revamp how purchases are made on the company website and the second would be a cybersecurity monitoring software for the corporate network.[6]

When meeting with the online software company, the attorney and the business specialist do most of the talking. The technology specialist asks various questions about the specifications and details of the program, but she mostly sees her role as one of implementation.[7] The business specialist confirms that the purchase price is satisfactory, and the attorney negotiates the specific language of any terms that they want included in the asset purchase agreement.[8]

---

[5] The "blockchain" is a technology protocol that creates a distributed ledger for all data transmissions across its network. It is best known for its affiliation with the cryptocurrency bitcoin, where all transactions of currency, in bitcoin form, are recorded in a public ledger. *See* Hossein Kakavand & Nicolette Kost De Sevres, *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*, SOC. SCI. RES. NETWORK 6 (Jan. 1, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251. What the reader needs to understand about the blockchain for the purposes of this Note is that it allows the transmission of data to be monitored and validated before being added to a chain of "blocks" of data that in total document the history of all data transmission on the blockchain network. *See id.*

[6] *See generally* William C. Anderson, *Comparative Analysis of Intellectual Property Issues Relating to the Acquisition of Commercial and Noncommercial Items by the Federal Government*, 33 PUB. CONST. L.J. 37, 43–46 (2003) (explaining what commercial software is and how it works); LYNETTE I. MILLETT, BARUCH FISCHHOFF & PETER J. WEINBERGER, FOUNDATIONAL CYBERSECURITY RESEARCH: IMPROVING SCIENCES, ENGINEERING, AND INSTITUTIONS 10, 15 (2017).

[7] *See Blockchain Under the Microscope*, ASSETMAN.NET (May 5, 2016), http://www.asset-man.net/n9044 (discussing the ideas of one of blockchain's technology specialists).

[8] *See generally* Danny Bradbury, *Can blockchain revolutionize online payments—and Canada's tech economy?*, FIN. POST (June 5, 2017), http://business.financialpost.com/entrepreneur/small-business/can-blockchain-revolutionize-online-payments-and-canadas-tech-economy

The team then gets together to set up the policies and procedures for the company's implementation of the software in their online sales platform. The business specialist informs the team that most of the company's online customers are individuals, so the application must be user-friendly. The attorney says that while they should keep user-friendliness in mind, it is crucial that the user know the terms of use for the website before contracting, because the company seeks to enforce California as their choice of law, even if the company sells to consumers around the country, and seeks to compel binding arbitration for any claims arising from the sale in order to minimize litigation costs.

The technology specialist says that in order to engage in transactions within the new software, customers will have to create and register an account number through the company's sales website. Therefore, in order to balance the user-friendliness desired by the business specialist with the need to have users know of the site's terms of use, she will add a link to the site's terms of use to the bottom of the webpage where users register their account numbers.

Finally, the team needs to set up policies and procedures for the use of the cybersecurity software on the corporate network. The technology specialist explains the technology's ability to track all data transmissions across the network and says that there are privacy concerns that some employees might have regarding that level of monitoring. Therefore, she recommends for the program to be implemented under the duties of the Chief Technology Officer ("CTO") or her designated subordinate.[9] She also suggests that the existing cybersecurity policies, developed by the technology department, be applied to this new program.[10] The others agree as they believe that the CTO would likely be more capable of using the program than anyone in their departments anyway.

With that hypothetical situation in mind, this Note will now examine the technical issues and legal problems that emerge from this exercise. First, it will discuss how the online contracts should have been crafted on the company's online sales platform and how the attorney's role should have been different in determining the technical layout of the website's

/wcm/450e776f-2df9-4da4-89a7-1e749f911965 (revealing the thoughts of a Canadian business specialist on the success rate of blockchain as opposed to bitcoin).

[9] *See* Colin Wood, *What is a Chief Technology Officer?*, GOV'T TECH. (July 29, 2016), http://www.govtech.com/people/What-Is-a-Chief-Technology-Officer.html (referring to "CTO's" as chameleons whose job varies depending on with which company they work).

[10] *Id.*

terms of use. Then this Note will discuss the legal issues of cybersecurity and how the attorney would need a greater role in the implementation and development of cybersecurity policies.

DISCUSSION

I. CONTRACT DRAFTING ONLINE HAS UNIQUE CHALLENGES, AND TO CONFRONT THEM, ATTORNEYS MUST UNDERSTAND THE PLATFORM THEY ARE USING AND THE SPECIALIZED REQUIREMENTS THAT HAVE DEVELOPED AROUND THE UNIQUE NATURE OF A WEBPAGE. TO PROPERLY PROTECT CLIENT INTERESTS, LAWYERS MUST ACTIVELY ENGAGE IN THE LAYOUT AND FORMAT OF THE CONTRACT, NOT JUST ITS CONTENT

Contracts are some of the most commonly utilized legal documents for lawyers.[11] No matter what branch of the law the attorney works in, it is almost certain that they have signed a contract for their employment at some point or drafted a contract to employ an assistant, an associate, or even the janitorial staff. But offline, attorneys have traditionally only had to concern themselves with the content of the contract—not necessarily the presentation or the platform from which it is accessed.[12]

Despite the ubiquity of contracts, online contract law has evolved in a way that seems markedly different from contracts offline.[13] Companies who quite clearly can afford to have attorneys look over their contracts, have fallen short of the standards that have been articulated by courts.[14] As will be discussed below, courts have formulated an instructive

---

[11] *See* John Kessel, *Common Legal Documents*, EZINE ARTICLES (May 22, 2008), http://ezinearticles.com/?Common-Legal-Documents&id=1193760 (providing a list of common legal documents, most of which are types of contracts).

[12] *See* Chee Ho Tham, Pey Woan Lee & Yihan Goh, *Contract Law*, *in* SINGAPORE ACADEMY OF LAW ANNUAL REVIEW OF SINGAPORE CASES 2013 14 (Teo Keang Sood et al. eds., 2014) ("[P]erhaps the contribution that *Sembcorp Marine* makes to the existing jurisprudence on implied terms in fact is to show the difficulty of rationalizing [sic] this area of law through any overarching principle of interpretation.").

[13] *See generally* Aaron E. Ghirardelli, *Rules of Engagement in the Conflicts Between Businesses and Consumers in Online Contracts*, 93 OR. L. REV. 719 (2015) (discussing the evolution of online contract and determining how to assess the validity of such contracts).

[14] *See* Eric Goldman, *Courts Won't Bail You Out If You Can't Remember What Contract Terms You've Agreed To*, FORBES (July 12, 2013), https://www.forbes.com/sites/ericgoldman/2013/07/12/courts-wont-bail-you-out-if-you-cant-remember-what-contract-terms-youve-agreed-to/#698089387fc8.

guide for attorneys to follow when dealing with the formation of contracts online. This Note will also show that the hypothetical attorney should have engaged more forcefully in discussions about the layout of the webpage in order to safeguard the client's legal interests in the contract terms.

A. Specht v. Netscape provides a good framework from which attorneys can formulate contracts online because it provides clear requirements for assent based upon the technical abilities of webpages

At the broadest level, *Specht v. Netscape* is about the enforceability of an online contract.[15] But the case provides a good framework from which lawyers can work to secure clients' rights under online contracts because it compares the enforceability of "clickwrap"[16] and "browse-wrap"[17] agreements. In 2002, the Second Circuit Court of Appeals affirmed that the mandatory arbitration provision in Netscape's online contract terms was unenforceable because the provision was not subject to a mandatory, non-leaky click-through.[18] Netscape was not a company that one might expect to be in dire need of competent counsel regarding the nuances of online contract formation.[19] However, Netscape still failed to establish an enforceable contract in conjunction with every download of one of their pieces of software.[20] Comparatively, Netscape created a technical setup for other pieces of its software that formed an enforceable contract with the download.[21] This is pertinent to the discussion of this Note's hypothetical because the hypothetical contract also seeks to enforce a

---

[15] *See generally* Specht v. Netscape Comm. Corp., 306 F.3d 17 (2d Cir. 2002) (holding that plaintiffs, in acting upon defendants' invitation to download free software made available on defendants webpage, did not agree to be bound by the software's license terms, despite that plaintiffs necessarily would have been aware of the existence of such terms prior to executing the download).

[16] *See* Cheryl Preston & Eli McCann, *Unwrapping Shrinkwrap, Clickwrap, and Browsewrap: How the Law Went Wrong from Horse Traders to the Law of the Horse*, 26 BYU J. PUB. L. 1, 28–31 (2011).

[17] *See* Ghirardelli, *supra* note 13, at 728 (describing browsewrap agreements as a contract where, "[u]pon visiting a website, the user is presented with a hyperlink . . . [that] generally refers to 'Terms of Service' or 'Terms of Use.' Only by clicking on this hyperlink is the user directed to the contractual terms that regulate use of the website.").

[18] *See Specht,* 306 F.3d at 20–21.

[19] *See* Haywood Kelly, *What's $10 Billion to AOL?*, MORNINGSTAR (Apr. 5, 1999), http://news.morningstar.com/articlenet/article.aspx?id=741.

[20] *See Specht,* 306 F.3d at 36–38.

[21] *See id.*

browsewrap agreement, and *Specht* sets out a good framework for how the hypothetical attorney should have proceeded.[22]

So, how did Netscape let this happen? Well, in order to get software from the Netscape website, all but one plaintiff went to a webpage run by Netscape "that urged them to 'Download With Confidence Using SmartDownload!'"[23] Then, "[a]t or near the bottom of the screen facing plaintiffs was the prompt 'Start Download' and a tinted button labeled 'Download.' By clicking on the button, plaintiffs initiated the download of SmartDownload."[24] This was the browsewrap[25] contract mentioned earlier, and it closely mirrors the contract in our hypothetical.

Netscape was attempting to enforce contract terms for binding arbitration as they related to this plug-in program, but, like in this Note's hypothetical, there was no express click-through manifesting assent to the license agreement.[26] What's more, the request for web users to review SmartDownload's terms and conditions was at the bottom of the page,[27] so users would have needed to see the "Download" instruction before downloading the plug-in program by scrolling to the bottom of the page, reading the request, and then linking to another page in order to be familiar with the terms and conditions for SmartDownload.[28] Again, this parallels the scenario envisioned in our hypothetical.[29]

Once SmartDownload had been downloaded, the plaintiffs were prompted to install Communicator.[30] The court described the process necessary to complete the download of Communicator:

> [The plaintiffs] were automatically shown a scrollable text of that program's license agreement and were not permitted to complete the installation until they had clicked on a 'Yes' button to indicate that they accepted all the license terms. If a user attempted to install Communicator without clicking 'Yes,' the installation would be aborted. All five named user plaintiffs expressly agreed to Communicator's license terms by clicking 'Yes.'[31]

---

[22] *See* discussion *supra* pp. 4–6.

[23] *Specht*, 306 F.3d at 22.

[24] *Id.*

[25] *See* Ghirardelli, *supra* note 13, at 728.

[26] *See Specht*, 306 F.3d at 22.

[27] *Id.*

[28] *Id.* at 23.

[29] *See* discussion *supra* pp. 4–6.

[30] *Specht*, 306 F.3d at 23.

[31] *Id.* at 21–22.

The court referred to this as "clickwrap," or more descriptively, as a "Mandatory, Non-Leaky Click-Through."[32] It is "mandatory" because it must be done in order to complete installation.[33] It is "non-leaky" because any attempt to circumvent it will terminate the installation.[34] And it is a "click-through" because it requires the user to click to expressly assent to all contract terms.[35]

Now, it is also worth noting that some contract terms available via browsewrap have been enforced by courts.[36] However, most of these courts have been dealing with cases where an entity-plaintiff had sufficient actual or constructive knowledge of the terms at issue.[37] But that is not relevant in analyzing our hypothetical, because the majority of consumers are individuals. That being said, attorneys should be cognizant that the requirements for online contracts may change depending who the other party is in the client's contract.[38]

B. Rather than settling for a browsewrap link to the website's terms of use, the attorney in our hypothetical should have insisted on a clickwrap agreement

Lawyers, especially those who focus on business issues, have a reputation among their business and technological colleagues for "throwing cold water" on exciting new ventures.[39] As such, it would be understandable that there may be a hesitancy for our hypothetical attorney to insist

---

[32] Goldman, *supra* note 14.

[33] *See Specht*, 306 F.3d at 24.

[34] *See generally id.* (discussing the nature of clickwrap and its importance in the digital word of the legal profession).

[35] *See id.* at 24.

[36] *See, e.g.*, Ticketmaster L.L.C. v. RMG Tech. Inc., 507 F. Supp. 2d 1096, 1107 (C.D. Cal. 2007).

[37] *See* Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 937–38 (E.D. Va. 2010) ("Most courts which have considered the issue [of browsewrap] . . . have held that in order to state a plausible claim for relief based upon a browsewrap agreement, the website user must have had actual or constructive knowledge of the site's terms and conditions, and have manifested assent to them."); *see also* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 472 (2006) ("An examination of the cases that have considered browsewraps in the last five years demonstrates that the courts have been willing to enforce terms of use against corporations, but have not been willing to do so against individuals.").

[38] *See When Lawyers Get in the Way*, ST. AUGUSTINE L. GROUP (Mar. 27, 2015) [hereinafter *When Lawyers Get in the Way*], http://www.staugustinelawgroup.com/st-augustine-business-law-real-estate-wills-attorney-lawyer-contracts/businesslaw101.

[39] *See id.*

upon being actively engaged in the decision-making process in areas that are not traditionally within the purview of attorneys. Indeed, as the hypothetical demonstrates, there may even be an understandable tendency for the lawyers to initially chime in about the strict legal criteria and then let the business and technology specialists figure out the rest within the attorney's general guidelines rather than engaging fully in the decision-making process.[40] This could create issues if the business and technology specialists have only a tenuous grasp on the legal implications of a decision due to the difficulty that lay people often have sifting through legal jargon. It could also create scenarios where attorneys later have to justify in court poor legal decisions that could have been avoided had they engaged more heavily in the process and assuming they understood the technical capacity involved, which often comes across as gibberish to attorneys.[41]

In the above hypothetical, by being overly deferential to the business interest and putting as few impediments as possible between the customer and the deal or account (i.e., being "user friendly"), the attorney did not adequately safeguard the client's interest in the contract terms.[42] However, a diligent attorney would have developed a better understanding of the technological issues involved and would have been able to translate them into legal solutions demanding that assent be made expressly manifest before the "deal" was complete or the account created, even if it meant sacrificing a little user friendliness in the layout.[43]

In order to post an offer online and ensure that "a reasonably prudent offeree in plaintiff's position would necessarily have known or learned of the existence of the . . . [contract terms] prior to acting,"[44] a website's contract structurally requires a Mandatory, Non-Leaky Click-Through. From there, the user must click through the terms and manifest express assent for each term.[45] Assent by notice—that is to say, assent by

---

[40] *See* discussion *supra* pp. 4–6.

[41] *See, e.g.*, Lisa Needham, *The Legal Tech Audit Proves Lawyers Are Terrible at Technology*, THE LAWYERIST (Sept. 12, 2014), https://lawyerist.com/76189/lawyers-terrible-technology-audit-will-prove/.

[42] *See* discussion *supra* pp. 4–6.

[43] *See, e.g.*, Needham, *supra* note 41.

[44] Specht v. Netscape Comm. Corp., 306 F.3d 17, 30 (2d Cir. 2002).

[45] *See id.* at 29–30 (citation omitted) ("[C]licking on a download button does not communicate assent to contractual terms if the offer did not make clear . . . that clicking on the download button would signify assent to those terms[.]").

way of a browsewrap format—or performance is not sufficient for the hypothetical attorney.[46]

All of this is to say that attorneys must ensure that those designing the website are using technology that brings the user to a screen that requires the express manifestation of intent to be bound to the contract terms before they are given the benefit of their bargain.[47] In the opening hypothetical, this would have meant that the attorney should have worked with the technology specialist as she crafted the website to ensure that instead of having users set up account numbers with a link to the terms of use at the bottom of the page, the user would need to be brought to a screen before the account was set up that required the user to click-through the terms of use that are at issue.[48] This collaboration would be absolutely crucial for the technology specialist to creatively craft the website design in a way that was still user-friendly.[49] User-friendliness is important because the concerns of the business specialist are valid. A business concerned with making a profit should be cognizant of the simplicity with which customers can use their website. But in order to protect the client interests—which, in this hypothetical, include the choice of law and binding arbitration provisions—the attorney must actively engage and "throw [a little] cold water"[50] on the discussions.

The one other quirk in need of translation from technical capacity to legal implication is that while the technology is there to create Mandatory, Non-Leaky Click-Throughs, attorneys should expect that controversies will arise expressly dealing the contract terms that were assented to by the user.[51] This is because a study in 2013 suggested that almost no individual online users access a website's terms of use when given the option, and of those who do, very few remain on the webpage long enough

---

[46] *See id.*

[47] *See id.* at 29 ("Mutual manifestation of assent . . . is the touchstone of contract.").

[48] *See* Fteja v. Facebook Inc., 841 F. Supp. 2d 829, 837 (S.D.N.Y. 2012) (explaining that clickwrap agreements that require the user to acknowledge and agree to the terms of service are generally upheld by circuit and district courts).

[49] The notion that creativity and ingenuity could overcome this problem, which has characterized the growth of the internet, is the subjective observation of this Note's author—not a sourced finding.

[50] *See When Lawyers Get in the Way*, *supra* note 38.

[51] *See generally* Yannis Bakos et al., *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1 (2014) (explaining how an overwhelming majority of consumers fail to read and understand standard form contracts prior to assenting to the terms therein).

to read the entire agreement.[52] In light of this and the fact that individuals are not held to browsewrap agreements,[53] there is a real and unsettled question of whether the courts are relaxing the duty to read for online contracts.

To insulate the hypothetical's client from this while still requiring a Mandatory, Non-Leaky Click-Through on the page where the account number would be created and registered, the attorney may want to insist that technical specialists require users to spend certain amount of time on the aforementioned page. The hypothetical's business specialists may balk at a policy like this, which would inconvenience customers when competitors have not done so. But it may be beneficial as a preventative measure that will keep clients ahead of courts' efforts to protect consumers. However, unlike in the case of determining whether clickwrap or browsewrap are the proper ways to secure contract terms, this would be a cautionary measure. That means the attorney would have more flexibility to work with the technology specialist to fashion such a practice in a way that meets the business specialist's concerns.

II. CYBERSECURITY LAW IS GROWING RAPIDLY AND CONTINUES TO TOUCH A VARIETY OF ESTABLISHED LEGAL FIELDS, AND AS SUCH, ATTORNEYS MUST ASSUME A GREATER ROLE IN THE DECISIONS THAT CLIENTS MAKE REGARDING CYBERSECURITY ISSUES AND IN THE IMPLEMENTATION OF SUCH DECISIONS

The legal news website, *Above the Law*, published a piece after the inauguration of now-President Donald J. Trump about areas of law that looked to be on a growth swing with the new administration in place.[54] In it, the author observed that "Privacy and Data Protection" is among the practice areas that will likely see significant growth.[55] Specifically, the author[56] opined that "[cybersecurity] is an area that simply has too much

---

[52] *See id.* at 1 ("[O]nly one or two out of every thousand retail software shoppers choose to access the license agreement, and most of those that do access it spend too little time to have read more than a small portion of the text.").

[53] *See* Lemley, *supra* note 37, at 472.

[54] Scott Mozarsky, *Practice Areas Positioned For Winning Under The Trump Administration*, ABOVE THE LAW (Feb. 14, 2017), http://abovethelaw.com/2017/02/practice-areas-positioned-for-winning-under-the-trump-administration/.

[55] *Id.*

[56] Perhaps critics would take this observation with a grain of salt since the author is the President of Bloomberg Law and BNA Legal Division, which sells access to law reports, including one on "Privacy and Security Law." *See About Us*, BLOOMBERG BNA, https://www.bna.com/scott-mozarsky-a17179885733/ (last visited Aug. 4, 2017).

activity, and too many open questions, to be anything but hot over the next four (or maybe forty) years."[57]

And it is easy to understand why there is so much growth in the field. From Target[58] to Yahoo,[59] there has been no shortage of high-profile data breaches of companies that people intuitively believe are large enough that they should have the means to protect themselves.[60] As one might expect, the law has taken an interest in the growing industry dealing with the security of such critically sensitive data.[61] But if, as *Above the Law* put it, the "open questions"[62] in cybersecurity law are going to be answered in a way that avoids the pitfalls that were shown in the development of online contract law—e.g. *Specht*—then attorneys advising clients need to understand the legal implications of the technical realities of cybersecurity.[63] This understanding cannot be limited to just those who will ultimately litigate these issues because crafting policies and procedures

---

[57] Mozarsky, *supra* note 54.

[58] *See* Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Board Room and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 643–45 (2015); *see also* Victoria C. Wong, *Cybersecurity Risk Management, and How Boards Can Effectively Fulfill Their Monitoring Role*, 15 U.C. DAVIS BUS. L.J. 201 (2015) (2013 Target data breach); Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, CAMACOL (Mar. 17, 2014), http://camacoltech.blogspot.com/2014/03/missed-alarms-and-40-million-stolen.html.

[59] *See generally* Sam Thielman, *Yahoo hack: 1bn accounts compromised by biggest data breach in history*, THE GUARDIAN (Dec. 16, 2016), https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached (describing the Yahoo data security breach); Brad Martorana, *Yahoo! Data Breach Results in Another Lawsuit Against Corporate Directors and Officers*, S&W CYBERSECURITY & DATA PRIVACY BLOG (Jan. 31, 2017), http://www.swlaw.com/blog/data-security/2017/01/31/yahoo-data-breach-results-in-another-lawsuit-against-corporate-directors-and-officers/ (describing the litigation stemming from the Yahoo data security breach).

[60] *See supra* notes 58–59 and accompanying text (discussing recent examples of high-profile data breaches occurring at large companies).

[61] *See, e.g.*, Raimund Genes, *Code Cyber: Preventing Breaches at Hospitals and Healthcare Practices*, 18 J. HEALTH CARE COMPLIANCE 13 (2016) (suggesting methods for health care organizations to address the threat of large-scale cyberattacks); Ariana L. Johnson, Note, *Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation*, 20 N.C. BANKING INST. 277, 297–308 (2016) (discussing cybersecurity legislation focused on information sharing practices).

[62] Mozarsky, *supra* note 54.

[63] *See* Specht v. Netscape Comm. Corp., 306 F.3d 17, 17 (2d Cir. 2002) (finding Netscape's arbitration agreement to be invalid because users did not knowingly assent to terms of the online agreement).

with a command of the technology involved will be helpful as courts then interpret such policies in conjunction with the developing law.

Below, this Note will discuss the threats posed by bad actors in the cybersecurity realm. It will then review the law that has cropped up around these threats, starting with a sampling of the statutes that govern how a client is to deal with a data breach by the threats discussed and ending with how negligence law has established a duty of care for sensitive data. All the while, this Note will look at how the attorney in the opening hypothetical should have engaged in the crafting of the company's cybersecurity policies and procedures in light of the threats posed and legal frameworks.

A. First, a review of cybersecurity fundamentals is necessary for all attorneys who advise clients facing cyber threats or holding sensitive digital information

Before one can understand the law that has thus far developed around cybersecurity, one must understand the fundamentals of cybersecurity. Specifically, one must understand the dangers that digital technologies are up against. And while most of the threats that will be detailed below fall under the heading of "cyber-crime," this Note will not focus on the criminal law aspects of the crimes, but will instead discuss what the hypothetical's attorney should keep in mind about the threats when crafting policies based on the laws addressed in the next section.

So, to start, there are a number of different threats that clients will face in the cyber realm. An exhaustive discussion of all of these would fill several books, so this Note will seek only to provide the level of understanding needed for our hypothetical attorney to competently contribute to the creation of policies and procedures. At the broadest level, the hypothetical's attorney creating policies for the blockchain-based cybersecurity system would need to be familiar with phishing attacks, spear phishing, advanced persistent threats, zero-day attacks, malware, ransomware, and spyware.[64] These will have some overlap. For example, an advanced, persistent threat may embed itself in a server through malware and then operate spyware until it can gain access to whatever it is targeting.

---

[64] *See generally* Ganesh Umapathy, *Evolution of Email Threats: The Rise of Ransomware, Spear Phishing and Whaling Attacks*, SONICWALL (Apr. 11, 2017), https://blog.sonicwall.com/2017/04/evolution-email-borne-threats/ (describing the many different types of cyber threats that exist).

But each is a distinct concept that our hypothetical's attorney should understand.

Phishing attacks are some of the most common forms of cyber attacks.[65] Phishing attacks are what many people associate with cyber-crime because nearly everyone has experienced a phishing attack.[66] But for those who do not know, phishing attacks are when bad actors send out myriad, seemingly indiscriminant emails that are designed to get unwitting recipients to click on a link or enter some kind of personal identifying information.[67] From there, the personal identifying information may be sold on less-than-reputable black-market sites,[68] or the link included may cause the computer to download malware or spyware.[69]

Phishing attacks are within a subset of what are known as "social engineering" attacks.[70] They manipulate social cues and prey on the psychology of the victim.[71] Many people reading this would probably conjure up the old, worn-out vision of a "Nigerian Prince" promising riches if the email recipient were to send money to help him until he comes into his crown.[72] But more often, phishing attacks that clients need to worry about are appeals to authority.[73] P.W. Singer and Allan Friedman, Brookings Institute scholars who have written extensively on the topic of cyber threats, described these appeals as follows:

> [These emails often] look like official e-mails from the victim's bank, employer, or some other trusted entity. They claim to require some action by the victim, perhaps to correct an account error or see a message on Facebook, and fool victims into visiting a web page where they are asked to enter their credentials. If the victim enters his or her account details, the attacker can now

---

[65] P.W. SINGER & ALAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 40 (2014).

[66] *See generally id.* (explaining that phishing is a common cyber-attack).

[67] *Id.* at 40–41.

[68] *See, e.g.*, Brian Krebs, *Shopping for W2s, Tax Data on the Dark Web*, KREBSONSECURITY (Jan. 31, 2017), https://krebsonsecurity.com/2017/01/shopping-for-w2s-tax-data-on-the-dark-web/.

[69] *See* SINGER & FRIEDMAN, *supra* note 65, at 58.

[70] *See id.* at 40.

[71] *Id.*

[72] *See generally The Nigerian Prince: Old Scam, New Twist*, BETTER BUS. BUREAU, http://www.bbb.org/new-york-city/get-consumer-help/articles/the-nigerian-prince-old-scam-new-twist/ (last visited Aug. 8, 2017) (describing the many different Nigerian scam letters that trick people into giving up personal information).

[73] *See* SINGER & FRIEDMAN, *supra* note 65, at 40–41.

> do anything with that information, from transfer money to read confidential e-mails.[74]

The next threat that clients face in the cyber realm, which our hypothetical's attorney should understand, are spear-phishing attacks. Like regular phishing attacks, these are within the umbrella of social engineering attacks.[75] But, rather than having a blanket email sent out to thousands or millions of people, spear phishing attacks target specific individuals and attempt to trick them specifically into falling for carefully individualized phishing emails.[76] At its core, spear phishing is described as "malicious messages tailored to individuals in order to appear legitimate, which are used to infect a specific target."[77]

Spear-phishing attacks require planning and information gathering.[78] As these attacks typically need to be highly customized to the individual that they are attempting to have fall victim to their attack, the costs of orchestrating a successful spear-phishing attack are substantial. As such, it is typically only going to be "big fish" that are targeted for spear phishing attacks.[79] For this reason, some cybersecurity industry specialists have begun referring to this type of attack as "whaling."[80]

And while the distinctions between these specialized attacks and general phishing are important for attorneys advising individuals and entities on cybersecurity law to know, the differences between the two attacks are more stylistic than technological.[81]

So, the attorney in this Note's opening hypothetical needs to keep in mind that phishing and spear-phishing attacks are not stopped by the program that he and the team are tasked with creating policies and procedures for. Rather, the program would create a ledger of data transmissions that

---

[74] *Id.*

[75] *See id.*

[76] *See generally* John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 400–01 (2016) (explaining that spear phishing involves customized emails).

[77] Karen Painter Randall & Steven A. Kroll, *Getting Serious about Law Firm Cybersecurity*, 2016 N.J. L. 54, 55.

[78] SINGER & FRIEDMAN, *supra* note 65, at 41.

[79] Caroline Fehr et al., *Computer Crimes*, 53 AM. CRIM. L. REV. 977, 986 (2016).

[80] *See, e.g.*, Daniel Garrie & Michael Mann, *Cyber-Security Insurance: Navigating the Landscape of a Growing Field*, 31 J. MARSHALL J. INFO TECH. & PRIVACY L. 379, 388 (2014).

[81] *See generally* Fehr et al., *supra* note 79, at 985–86 (explaining the different types of phishing attacks).

would show what data was brought onto the corporate network by the attack. The attorney would also need to keep in mind the training, which employees would receive for operating the blockchain-based program, as this training should include information regarding how to spot and avoid attempted social engineering and manipulation on the network.[82]

The next cybersecurity dangers that the hypothetical's attorney needs to understand in order to properly advise his client are advanced persistent threats ("APTs").[83] Much like spear-phishing attacks, APTs are often used by sophisticated bad actors since they require a greater input of time and resources.[84] These are some of the most poorly understood threats looming in cyberspace, largely because they require advanced coding and computational skills to pull off successfully.[85] However, one does not need a Ph.D. in Computer Science to understand the threat that APTs pose to clients:

> An APT is a multi-step attack designed to infiltrate a system and remain there undetected for a long period of time to obtain high-value information. Common cyberattack methods, such as phishing emails, are often the first step in the multistep process, but under an APT attack, the perpetrator will focus on its target until it finds a way into the system. Attacks are adapted in response to the level of success or failure with which they affect a target organization.[86]

Typically, an APT will find its way into the targeted system through some means other than an overt attack.[87] Spear-phishing is often how the initial software is introduced,[88] but it could be introduced through more conventional means, as well.[89] What sets APTs apart is that rather than trying to gather any and all information that might be of value, APTs have

---

[82] *See generally What is Malware and How to Defend Against It?*, KASPERSKY LAB, https://usa.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it#.WMW6kfnytPY (last visited Aug. 15, 2017) [hereinafter *What is Malware?*] (explaining what malware is and how to best protect against malware attacks).

[83] *See generally* SINGER & FRIEDMAN, *supra* note 65, at 55–60 (describing advanced persistent threats and how to deter them).

[84] Chris Laughlin, Note, *Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations are Effective*, 14 COLO. TECH. L.J. 345, 353 (2016).

[85] *Id.*

[86] *Id.*

[87] *Id.* at 352–53.

[88] Sharon D. Nelson, *Cloud Security Alliance Warns of the "Treacherous 12" Cloud Computing Threats*, 27 S.C. L. 8, 8 (2016).

[89] *Id. See also* Daniel Terdiman, *Stuxnet Delivered to Iranian Nuclear Plant on Thumb Drive*, CNET (Apr. 12, 2012), https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/ (explaining methods used to conduct cyberattacks).

a specific target and may lie in wait until they have gathered the information necessary to access, extract, and deliver that target to whoever designed the APT.[90] APTs may conceal themselves, and they may be hiding on a system for an extended period until it seeks its opportunity.[91]

Additionally, the attorney in our hypothetical needs to understand clients' vulnerabilities to zero-day attacks. Zero-day attacks are perhaps best categorized as a subset of or complement to APTs.[92] These attacks exploit "software vulnerabilit[ies] that [are] unknown to the computer user and software manufacturer"[93] in a system's hardware or software.[94] So for the affected system, the day the attack happens is day-zero of knowing that the vulnerability exists.[95] Now, not all of these are discovered by the attackers.[96] In fact, "most attacks attempt to exploit vulnerabilities that the vendor has already discovered and attempted to ameliorate via a code update or 'software patch.'"[97] Unfortunately, "many users don't always pay attention to these security updates and leave the vulnerabilities unpatched."[98]

What the hypothetical's attorney would need to keep in mind with regard to these advanced threats is that the blockchain-based program would trace exactly what data was transmitted.[99] Therefore, if the policies and procedures developed to detect breaches—which will be discussed in greater depth below with respect to negligence doctrines—find the breach before it has found a way to execute its attack, there must be policies in place for how to take the threat off the network.[100] The attorney should also consider the benefits of sharing information agreements with other entities so they don't fall victim to the same attack and so the client has access to a greater knowledge base of threats to be on the lookout for.[101]

---

[90] *See* SINGER & FRIEDMAN, *supra* note 65, at 56.

[91] *See id.* at 58.

[92] This is how this Note's author thinks of zero-day attacks, but it is not necessarily a recognized subcategory.

[93] Paul Stockton & Michael Golabek-Goldman, *Curbing the Market for Cyber Weapons*, 32 YALE L. & POL'Y REV. 239, 240 (2013).

[94] *See id.*

[95] *See id.*

[96] *See id.* at 240–41.

[97] SINGER & FRIEDMAN, *supra* note 65, at 62.

[98] *Id.*

[99] *See* Johnson, *supra* note 61, at 278.

[100] *See id.* at 63–64.

[101] *See id.* at 301–02.

Now, we move from the method of the threats posed in the cyber realm to the actual software that is used to orchestrate these attacks. Malware is a term used to describe "malicious software."[102] This can refer to everything from a computer virus that comes onto a system through a phishing email to highly complex software.[103] Malware is a piece of software that is designed to perform a task before it reaches the victim's computer, which damages the victim and benefits the designer, should the victim allow the software onto his or her computer, network, or hardware.[104]

Next, ransomware is software that takes control of an operating system, server, or other critical piece of hardware and demands payment to the designer of the ransomware as ransom for getting back control of one's hardware.[105] Ransomware is often thought of as a type of malware, but it is different than malware in that it has become a distinct type of cybercrime.[106]

And finally, spyware is software that monitors the behavior of a computer or system user.[107] It may be used in conjunction with other attacks to maximize the effectiveness of those other threats.[108]

The main thing that attorneys would need to have in mind regarding malware and its ransomware/spyware variants would be that they are the actual programs that the cybersecurity program would be on the lookout for.

B. Next, a review of the law that has already cropped up around cybersecurity issues will reveal how the hypothetical attorney should have collaborated with the technology specialist on decisions regarding the governance and implementation of the cybersecurity program

---

[102] *See generally What is Malware?*, *supra* note 82 (explaining malware and the ways to protect against it).

[103] *Id.*

[104] SINGER & FRIEDMAN, *supra* note 65, at 43.

[105] *See generally Ransomeware & Cyber Blackmail*, KASPERSKY LAB, https://usa.kaspersky.com/internet-security-center/definitions/ransomware#.WMW7PfnytPY/ (last visited Sept. 10, 2017) (explaining what Ransomware is and the dangers behind it).

[106] *See generally What is Cybercrime: Risks and Prevention*, KASPERSKY LAB, https://usa.kaspersky.com/resource-center/threats/cybercrime (last visited Sept. 10, 2017) (describing what cybercrime is and the different ways to commit a cybercrime).

[107] *See generally What is Spyware?—Definition*, KASPERSKY LAB, http://usa.kaspersky.com/internet-security-center/threats/spyware#.WMW7wvnytPY (last visited Sept. 10, 2017) (describing spyware's purpose and how it can gain access to personal information).

[108] *Id.*

There are many routes through which victims of cybersecurity breaches can find their ways into legal trouble. For example, the Health Insurance Portability and Accountability Act of 1996 (commonly known as "HIPAA") governs the privacy and cybersecurity requirements of the healthcare industry.[109] Also, violations of the rules governing confidentiality are prominent in the legal field.[110] However, since this Note's hypothetical focuses on the role of the attorney, it will focus on the two most generally applicable ways in which a failure of cybersecurity has resulted in legal problems: data breach statutes and negligence.

At their broadest level, data breach statutes are state laws that have been passed in all but two states: Alabama and South Dakota.[111] There are numerous variations on a general theme that substantial breaches and disclosures of personally identifying information will require that the victims of the breaches be notified that the security of this data has been compromised.[112] Statutory violations may also result in fines or other liabilities associated with the breach.[113]

There is plenty of literature discussing data breach statutes.[114] So rather than regurgitating the findings of myriad others on this topic, this Note will endeavor to focus on three specific states, which together give a good sampling of the direction in which the law seems to be heading on the issue of disclosure requirements for breaches in data privacy. Those

---

[109] *See* Kenneth M. Siegel, *Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 PENN ST. L. REV. 779, 794–95 (2007).

[110] *See* MODEL RULES OF PROF'L CONDUCT r. 1.6 (AM. BAR ASS'N 2014) (explaining when a lawyer has a duty of confidentiality, versus when he has a duty to disclose information); *see also id.* cmt.18 (describing factors and reasons when a lawyer should be confidential and when a lawyer can disclose information).

[111] *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Feb. 24, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[112] *See id.*

[113] *See generally* Abraham Shaw, Note, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517, 560 (2010) (discussing how violators of breach security statutes should have repercussions).

[114] *See generally* Yasmine Agelidis, *Protecting the Good, the Bad, and the Ugly: "Exposure" Data Breaches and Suggestions for Coping with Them*, 31 BERKELEY TECH. L.J. 1057 (2016) (discussing how to deal with data breaches); Hilary G. Buttrick et al., *The Skeleton of a Data Breach: The Ethical and Legal Concerns*, 23 RICH. J.L. & TECH. 1 (2016) (discussing the issue and increase in data breaches); Shaw, *supra* note 113 (discussing how one can ensure notification of a data breach, as well as how one can protect himself from a data breach).

states will be California, Florida, and Massachusetts. So, while the hypothetical's contract had a choice of law provision specifying California as the governing state, this Note will also explore how Florida's and Massachusetts's statutes would structurally affect the attorney in the hypothetical scenario.

There are five general topics to consider when dealing with a data breach statute: (1) the definition of "breach"[115] and what data the breach applies to;[116] (2) the times when notification is required;[117] (3) the threshold at which alternative means of notification can be used;[118] (4) the threshold at which governmental agencies must be informed of the breach;[119] and (5) the liabilities that can be imposed for a breach.[120] Now, the third and fourth topics are pretty uniform amongst the state statutes that this Note will delve into, so they will not be its focus.[121]

California has done a particularly good job flushing out all of these topics. In the California Civil Code, there is a general duty to disclose a "breach in the security" of a system that contains personal information regarding affected residents of California.[122] This duty is triggered "following discovery or notification of the breach in the security of the data."[123] However, encrypted data is exempted from the duty to disclose as long as the encryption key has not also been compromised.[124] California is also notable because it details what information must be included in the notification of the breach and even goes so far as to mandate particular headings

---

[115] *See* FLA. STAT. § 501.171(1)(a) (2014) (explaining the meaning of "breach" in regards to "breach of security").

[116] *See id.* § 501.171(1)(g) (defining "personal information").

[117] *See id.* § 501.171(3)–(4) (describing what is required when giving notice to the department and individuals in the event of a security breach).

[118] *See id.* § 501.171(4)(f) (explaining when "substitute notice" may be given in lieu of "direct notice").

[119] *See id.* § 501.171(6) (identifying when and how that notice must be given by third parties and third-party agents).

[120] *See id.* § 501.171(9) (explaining how violations of the statute are enforced).

[121] *See generally supra* notes 116–17.

[122] *See* CAL. CIV. CODE § 1798.82(a) (2017).

[123] *Id.*

[124] *See id.*

to be used in the notification.[125] These headings include: "'What Happened,' 'What Information Was Involved,' 'What We Are Doing,' 'What You Can Do,' and 'For More Information.'"[126]

California also has a fairly broad view of what personal information triggers the duty to notify.[127] Specifically, the subtitle dealing with breaches defines personal information as "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual."[128] The definition then enumerates a non-exhaustive list of over a dozen categories of data that could be categorized as "personal information," which includes minor information, such as a name or physical description, alongside critically sensitive information, such as a resident's social security number.[129]

California's notification must come within "the most expedient time possible and without unreasonable delay."[130] The only reasonable delay spelled out in the statute deals with the needs of law enforcement,[131] although other delays could conceivably be argued as "reasonable." But overall, California sets a relatively high watermark of strict requirements for the definition of breach, as well as the timeframe in which the notifications must be sent out.[132]

Finally, California is probably the friendliest state this Note will examine from a consumer perspective for the above reasons, but also because a private cause of action is created for reckless, willful, or intentional violations of the duty to disclose. These violations are capped at $3000 per incident,[133] while negligent violations are capped at $500 per incident.[134]

So, under the California law—the law specified in the hypothetical website's terms of use—the hypothetical's attorney would want to take advantage of the continuous monitoring of data transmissions by the

---

[125] *See id.* § 1798.82(d)(1) (identifying the notification requirements in the event of a security breach).

[126] *Id.*

[127] *See id.* § 1798.80(e) (defining "personal information").

[128] *Id.*

[129] *Id.*

[130] *Id.* § 1798.82(a).

[131] *Id.*

[132] *See generally id.* § 1798.82(a) (providing the timeframes in which the consumer should be notified); § 1798.82(g) (providing the definition for a "breach of the security of the system").

[133] *See id.* § 1798.84(c).

[134] *See id.*

blockchain-based cybersecurity program in order to know precisely when a breach has occurred. However, he would also need to be aware that the "discovery or notification of the breach in the security" will be expedited when they have a system that allows the corporation to discover breaches in real time on the ledger of data transfers.[135] So, if phishing, spear-phishing, APTs, or zero-day attacks were used to transfer a piece of malware onto the network to breach the personal information of consumers, then the hypothetical's attorney would need to know that the company had the software and ability to near-instantly discover the breach.

This in turn would mean that a legal team would need to be more involved in the implementation of the security program in order to get the disclosure procedures started as soon as possible. What is more, in order to quickly determine "What Happened" and "What Information Was Involved,"[136] the legal team would need quick access to the record of the data being transferred over the network. As such, the hypothetical's attorney may have wanted to insist that either the program be jointly administered by the technology and legal departments or that a Chief Information Security Officer ("CISO")[137] be designated to administer the program. This CISO would be tasked with coordinating between all relevant departments.[138]

Regarding the actual information that would be breached in this Note's hypothetical, the attorney would want to insist that some proactive steps were taken to itemize and inventory the data that was kept on the company's network. In particular, the attorney would want to know if measures currently existed that categorized data that contained "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual."[139] This would be critical if the company were operating under the pressing but ill-defined time constraints imposed by California law.[140]

By contrast, Massachusetts has a more forgiving statutory regime from the perspective of the breached entity. Massachusetts still requires a

---

[135] *See id.* § 1798.82(a).

[136] *Id.* § 1798.82(d)(1) (internal quotation marks omitted).

[137] *See generally* Wood, *supra* note 9 (describing the role of a Chief Information Security Officer as a leader in cybersecurity in an organization).

[138] *See id.* (detailing the various functions performed by a Chief Information Security Officer, in light of the fact that a CTO "does not have a standard definition.").

[139] CAL. CIV. CODE § 1798.80(e) (2017).

[140] *Id.* § 1798.80(a)–(c).

general duty to notify residents about breaches in the security of their unencrypted or decryptable personal information.[141] However, in Massachusetts a "[b]reach in security" only applies to data that "creates a substantial risk of identity theft or fraud against a resident of the commonwealth."[142] So in Massachusetts, while there is still the general duty to notify residents that their personal information may have been accessed, the personal information that is at issue must be sufficient to independently create a "substantial risk" that the resident's identity could likely be stolen or defrauded with the breached information.[143] This means that minor descriptors of a consumer may not trigger the notification requirements in Massachusetts that would be triggered in California.[144]

Massachusetts also distinguishes itself from California by not creating a private cause of action for residents, should a breached entity not comply with the statutory requirements.[145] Rather, Massachusetts imposes a civil fine that may not exceed $100 per affected individual.[146]

So if the hypothetical's attorney planned to operate under a Massachusetts-type statute, he would still want to make sure that data had been identified as potentially "personal information."[147] However, because the penalty for not complying with the notification requirements is only $100 per affected individual, he may be more willing to craft policies that that reflect the differing risk of exposure.[148] For example, the attorney should consider balancing the privacy concerns for employees that were expressed by the technology specialist by allowing the technology department to be the only ones with direct access to the ledger created by the blockchain. But this should have the caveat that when there is a breach of personal information, the technology specialists will deliver a copy of the

---

[141] *Id.* at § 3 (identifying the "[d]uty to report [a] known security breach or unauthorized use of personal information"). *See generally* MASS. GEN. LAWS ch. 93H, § 1(a) (2007) (providing definitions for "Security Breach" laws).

[142] *See id.* § 1(a) (defining "[b]reach of security") (internal quotation marks omitted).

[143] *See id.*

[144] *Compare* MASS. GEN. LAWS ch. 93H, § 1(a) (2007) (stating that there must be a "substantial risk" prior to notifying the consumer), *with* CAL. CIV. CODE § 1798.82(a) (2017) (requiring notification if there is mere reasonable belief that personal information could have been compromised).

[145] *Compare* MASS. GEN. LAWS ch. 93I, § 2 (2007) (imposing a civil fine for violating the statute), *with* CAL. CIV. CODE § 1798.84(c) (2017) (creating a private cause of action for customer).

[146] *See* MASS. GEN. LAWS ch. 93I, § 2 (2008).

[147] *See id.*

[148] *See id.*

relevant portion of the ledger to the legal department as quickly as possible.

And if Massachusetts is more forgiving than California in its definitions of breach and personal information, Florida would likely be seen as being even more so.[149] This is because while Florida law still creates a general duty to notify consumers when their personal information has been breached,[150] Florida's statute defines "personal information" even more narrowly than Massachusetts' statute. Specifically, Florida law defines personal information as the name of the victim *and* any of the following: the individual's social security number; the identification number on an individual's government-issued document used to verify identity; the "financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account";[151] medical information of the individual; or individuals' identification number for their health insurance policies.[152] Disclosure of an individual's email address along with information sufficient to access the email account is also considered "personal information."[153]

Florida's statute is also notable for a few other reasons. The first is that it gives a clear timeline for sending notifications out to affected residents.[154] Under the Florida statute, notification must be given within 30 days of the breach.[155] Another 15 days may be granted for "good cause," which is left undefined.[156] Florida also specifies certain information that must be included, but it does not go so far as California, as to mandate certain headings.[157] But what is particularly notable in the Florida statute is that there is an explicit requirement that affected entities take "reasonable measures" to secure their electronic data.[158]

---

[149] *See generally* FLA. STAT. § 501.171(1)(a), (g) (2017) (defining "breach of security" and "personal information").

[150] *See id.* § 501.171(4)(a).

[151] *See id.* § 501.171(1)(g)(1)(a)(III).

[152] *See id.* § 501.171(1)(g)(1)(a)(IV)–(V).

[153] *See id.* § 501.171(1)(g)(1)(b).

[154] *See id.*

[155] *See id.*

[156] *See id.*

[157] *See id.* § 501.171(3)(b)(1)–(5).

[158] *See id.* § 501.171(2).

So, under Florida law, the hypothetical's attorney would have more flexibility than he would under Massachusetts and certainly California law. The personal information that would need to be inventoried could be very specific and only related to the enumerated list given in the statute.[159] What is more, the legal department could create very clear guidelines as to when the technology specialists would need to bring in the legal team. With the default 30 day deadline,[160] the hypothetical's attorney and technology specialist could establish a policy that would allow the technology specialist seven days after a breach to organize and establish exactly what happened without the time pressure of a statute like California.[161]

The hypothetical's attorney would also need to think about what constitutes "reasonable measures,"[162] which brings us to the second area of law that is of particular note in cybersecurity law: negligence. Negligence as a doctrine for liability in cybersecurity exists regardless of what data breach statute is applicable.[163] Instead, whether our hypothetical's company negligently handles sensitive information revolves around whether or not the company took "due care" or "reasonable care."[164] And in the realm of cybersecurity, the National Institute of Standards and Technology ("NIST") has put forth a framework for identifying reasonable steps to safeguard data.[165] This framework emerged as a result of an executive order[166] and is now the standard by which an entity's reasonableness or negligence is increasingly being measured.[167]

---

[159] *See id.* § 501.171(1)(g)(1)(a)(IV)–(V).

[160] *See id.* § 501.171(3)(a).

[161] *See, e.g.*, CAL. CIV. CODE § 1798.82 (2017) (describing the urgency of notifying consumers about security breaches).

[162] *See* FLA. STAT. § 501.171(2) (2017).

[163] *See* RESTATEMENT (SECOND) OF TORTS § 281 (AM. LAW INST. 1965) (discussing the doctrine of negligence as a cause of action in tort).

[164] *See id.* § 283.

[165] *See* NAT'L INST. STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 4–5 (2014) [hereinafter NIST], https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[166] *See* Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

[167] *See* Danielle Gilmore & David Armillei, *The Future is Now: The First Wave of Cyber Insurance Litigation Commences, and the Groundwork is Laid for the Coming Storm*, ASPATORE, 2016 WL 1089828, at *5 (Feb. 2016) (stating that policies following the NIST framework "are becoming ever more common, and are creating a baseline by which 'reasonable' behavior . . . may be judged in the future.").

But before this Note delves into NIST and how the hypothetical attorney could use the framework to craft cybersecurity policies that protect the client company from negligence actions in the event of a breach in the company's data, it is worth noting that NIST is not without criticism overall.[168] Specifically, the NIST framework may focus too heavily on how the private sector regulates itself for security purposes.[169] By contrast, NIST may be found lacking from a policy perspective for failing to offer incentives for private actors to adopt more rigorous defenses.[170] However, the flexibility of the NIST framework, the ease of understanding and implementing its functions, and a developing consensus that the NIST framework should be the baseline for reasonable care in negligence actions[171] all lead this Note to argue that it is the best baseline for attorneys seeking to advise clients in decisions around cybersecurity technology, as is the case for our attorney in the opening hypothetical.

The NIST framework involves five "functions" that should be followed, and within those five functions, efforts should be made to create physical, technological, and administrative safeguards against a breach for each function.[172] Those five functions are: Identify, Protect, Detect, Respond, and Recover.[173]

The Identify function establishes what data is particularly at risk and adopts a risk-based approach to defending that data against cyber attacks.[174] To do this, NIST suggests that the entity seeking to ensure the security of its data focus on asset management, business environment, governance, risk assessment, and risk management.[175] Asset management

---

[168] *See* Scott Shackelford et al., *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217 (2016) (comparing the NIST framework with other "Bottom-Up" cybersecurity structures around the world).

[169] *See id.* at 256.

[170] *Id. See generally* David Inserra & Steven P. Bucci, *Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, HERITAGE FOUND. (Mar. 6, 2014), http://report.heritage.org/bg2880 (suggesting that the U.S. government should promote a private-sector system for securing and accrediting technology companies).

[171] *See* Gilmore & Armillei, *supra* note 167, at *5; *see also* Scott Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 336 (2015) (stressing the benefits of applying the NIST Framework).

[172] *See* NIST, *supra* note 165, at 4–5, 7–9.

[173] *Id.* at 4.

[174] *See id.* at 8, 20–23.

[175] *See id.* at 19.

means that "[t]he data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent[ly] with their relative importance to business objectives and the organization's risk strategy."[176] Business environment includes cultivating a business culture that prioritizes goals and objectives and that uses such prioritization to inform cybersecurity decisions.[177] Governance deals with having policies that govern who can access certain data.[178] Risk assessment means that the data an entity holds has been analyzed and that information has been used to prioritize the most sensitive or vulnerable data.[179] And risk management means having a cyber-insurance strategy.[180]

So, to meet the reasonableness standard under the NIST framework, the hypothetical's company must have the team construct a plan and policy structure in proportion to their middling sophistication that identifies the most vulnerable data and adopts a risk-based approach to protect them. This would include controlling the assets that are used to access an entity's data both in the physical world by controlling access to the network servers, and in the digital world by imposing technological controls by which network users have authorization only to particular data. Meeting the reasonableness standard would also mean promoting a culture of security within the entity.[181] Governing policies should be in place to make sure that individuals only have access to the amount of data that is necessary to fulfill their duties.

These steps should be taken with the goal of implementing them for every person who works for the hypothetical company, from the CEO to the entry-level analyst.[182] With regard to the particular program in the opening hypothetical, meeting the reasonableness standard for the Identify function could look like using the ledger to create real-time documentation of the data that is available. The legal team could craft a policy requiring

---

[176] *Id.* at 20.

[177] *Id.* at 21.

[178] *Id.* at 21–22.

[179] *Id.* at 22–23.

[180] *Id.* at 23.

[181] *See generally* Shackelford et al., *supra* note 168, at 336 (discussing a hypothetical company's implementation of the NIST framework to meet the reasonableness standard).

[182] *See id.*

the technology specialists to have metatags[183] on all data to show where it has been stored at various points after being transmitted from one account to another. It could mean having a regularly scheduled review of the ledger of data transmissions by the Chief Legal Officer and Chief Technology Officer, to ensure that the information is being used to create risk-based policies throughout the cybersecurity framework.

The Protection function is the function that most people think of when they envision "cybersecurity." It is the defensive policies, controls, and technologies that are meant to keep a breach from happening.[184] NIST suggests that this function focus on access controls, training, data security, administrative procedures, maintenance, and protective technologies.[185] Access controls are exactly what they sound like: controlling and minimizing the access that individuals have to sensitive data while still allowing them to perform their functions.[186] Likewise, training is exactly what it sounds like: training employees and other stakeholders to avoid falling for common social engineering attacks, such as phishing.[187] Data security, while seeming to be a catch-all, actually refers to the need to implement the risk-based approach established by the Identification functions when dealing with protection of the data.[188] Administrative procedures refer to the need to craft policies and protocols that enable and encourage all of the other physical and technological protections of the data.[189] Maintenance refers to the need to keep all of the protection measures up-to-date in the quickly evolving world of cybersecurity.[190] And protective technologies refers to the use of defensive capabilities,[191] such as firewalls[192] or air-gaps[193] to prevent a breach.

---

[183] *See generally* Roland Knaak, *Metatags and Keywords as comparative advertising*, 9 J. INTELL. PROP. L. & PRAC. 770, 770 (2014) (describing metatags as "features of the digital environment that are invisible to internet users, but which are recognized by internet search engines and therefore frequently used as instruments in competition.").

[184] *See* NIST, *supra* note 165, at 8.

[185] *Id.*

[186] *Id.* at 23–24.

[187] *Id.* at 24–25.

[188] *Id.* at 25–26.

[189] *See id.* at 26–28.

[190] *Id.* at 28–29.

[191] *Id.* at 29–30.

[192] SINGER & FRIEDMAN, *supra* note 65, at 62.

[193] *Id.* at 63.

So to meet the NIST reasonableness standard with respect to the Protection function, the hypothetical's attorney would need to establish the risk-based approach that the team developed in the Identification function of their data. With that as the context, the client would then need to craft policies and protocols, including training and the use of innovative technologies. The combination of training and technologies is designed to minimize the risks of both social engineering attacks, as well as the more technical attacks. It is also important that the attorney advises the client to keep meeting the reasonableness standard and to develop plans that maintain their protective measures on an ongoing basis. The hypothetical's attorney should also recognize the overlapping nature of these functions, and how complying with one function sets the client up for success in complying with the next function.[194] This will prove to be a theme within the NIST framework.[195]

Using the NIST framework to find protective uses for the program in the opening hypothetical,[196] the attorney would want to periodically coordinate with the technology specialist to determine the threats that the company faced in the past. Then, the program would enable the legal department to craft training for all levels of the company based on the types of data that the program revealed they were most in contact with.[197]

The Detection function, which was mentioned briefly in the above discussion of APTs and zero-day attacks, establishes the ability to determine when a breach has taken place.[198] NIST recommends that Detection efforts focus on anomalies, continuous security monitoring, and detection processes.[199] A focus on anomalies means that the client should develop tools to ascertain when data has been accessed by an actor who would not normally access this data.[200] It also includes a need to investigate such

---

[194] *See* NIST, *supra* note 165, at 8.

[195] *See id.* at 19.

[196] *See generally* Lei Shen, *The NIST Cybersecurity Framework: An Overview and Potential Impacts*, 10 SCITECH L. 16, 18 (2014) https://www.americanbar.org/content/dam/aba/publications/scitech_lawyer/2014/summer/nist_cybersecurity_framework_overview_potential_impacts.authcheckdam.pdf (providing an explanation of the NIST framework).

[197] NIST, *supra* note 165, at 23–24.

[198] *Id.* at 30–31.

[199] *Id.* at 19.

[200] *Id.* at 30.

anomalies to determine whether the access was inappropriate or unauthorized.[201] Continuous security monitoring means that the client should incorporate techniques that allow for the information system and assets to be monitored regularly in order to identify "cybersecurity events" and ensure the "effectiveness of protective measures."[202] Finally, detection processes means developing policies and procedures that make it more likely that an unauthorized access of data is discovered in a timely manner.[203]

This means that in order for the hypothetical's attorney to get the company to meet the reasonableness standard for Detection, the attorney must focus on developing ways of discovering anomalous behavior and events within their system. Such a focus should include technological processes that allow for the continuous monitoring of their systems and administrative processes that enable swift detection. Here, the program that is immediately at issue would be particularly helpful. This will inevitably require cooperation with the technology specialists, but that cooperation cannot mean being overly deferential as the hypothetical attorney was. Rather, it must mean taking the legal issues that have been discussed above and using that knowledge to work with the technology specialists to tailor the most effective solutions to the most pertinent threats.

The Response function is to ensure that there is a plan in place for how the entity will react in the event of the detection of a breach.[204] This function should focus on formulating a response plan, communications, analytics, mitigation, and improvement.[205] The plan is designed to ensure that the client has a well thought out strategy for responding to the breach.[206] This should include complying with any data breach laws that

[201] *Id.* at 30–31.

[202] *Id.*

[203] *Id.* at 31–32.

[204] *Id.* at 33–34.

[205] *Id.* at 19.

[206] *Id.* at 33.

are applicable, as well as being cognizant of public relations and reputational concerns.[207] The plan should also focus on communicating.[208] The communications prong seeks to ensure that there are established means for getting the clients' messages out despite the breach.[209] Analytics, mitigation, and improvements must then work together in order to ascertain how the breach occurred; what steps may be taken to reduce the damage done by the breach; and how similar, future breaches may be avoided.[210]

So for the hypothetical's attorney to get his company to meet the NIST reasonableness standard with respect to the Response function, the legal team should have thought through how they would react should a breach occur. The attorney must plan ahead about who will execute response plans, and how (or whether) they will communicate their responses to the public, governmental agencies, as well as internally.

Inevitably, this would mean cooperating with the business specialists as well. Getting the business back up and running full speed will take both the legal expertise of the attorney, regarding how the company should navigate the issues presented by the negligence rules and data breach statutes, and the expertise of the business specialists, regarding exactly what data is necessary for resources to be diverted to most efficiently compensate for any damage caused by the breach.

There should also be a plan put in place in order to learn from the mistakes that resulted in the breach, in an effort to meet the reasonableness standard.[211] And this is where the hypothetical's attorney, who had the knowledge of technical threats faced by the company, would have been especially useful for his client because crafting policies and messages for the client that clearly articulate how the client is taking reasonable steps to

---

[207] *See id.*; *see also* CAL. CIV. CODE § 1798.82 (2017) ("A person or business that conducts business . . . and [who] owns or licenses computerized data[,] including personal information, shall disclose a breach of the security of the system following discovery or notification of the breach . . . ."); MASS. GEN. LAWS ch. 93H § 2(a) (2007) (setting forth the regulations necessary to safeguard residents' personal information); FLA. STAT. § 501.171(2)(h) (2017) ("Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.").

[208] *See* NIST, *supra* note 165, at 33.

[209] *Id.*

[210] *Id.* at 33–34.

[211] Kenneth C. Johnson & Dan Klein, *The February 2016 California Attorney General's Data Breach Report Sets a Standard for "Reasonable Security"—What Does This Mean for Cybersecurity Litigation?*, A.B.A. BUS. L. TODAY (May 2016), https://www.americanbar.org/publications/blt/2016/05/04_klein.html.

remedy the situation may be the best way to save the reputation and public impression of the client—not to mention potentially winning the goodwill of courts by providing clear, thoughtful, and reasoned responses based on a solid understanding of the issues at play.

Finally, the Recovery function is to make certain that the entity has a plan in place to get operations back on track after the breach has happened.[212] This, too, focuses on planning, improvements, and communications.[213] Specifically, there needs to be a plan in place to make concrete changes based upon the risks that revealed themselves during the breaching event.[214] These changes can be improvements to the technology, to the physical access, or even to the administrative policies that are in place.[215] Most importantly, the client needs a plan identifying how the changes should be communicated both internally, to maintain training, and externally, to protect the reputation of the client.[216]

CONCLUSION

The attorney in the opening hypothetical came at his assignment with a traditional legal attitude. He handled the contract language, but he deferred to the technology and business specialists on technology and business issues. Intuitively, there would seem to be nothing wrong with that. But as new technologies continue to encroach into more and more areas of life and the economy, it is inevitable that the law around these technologies will continue to grow as well. And as it does, it will be critical that attorneys actively engage in the decisions that their clients make regarding these technologies in order to safeguard those clients' interests.

---

[212] MICHAEL BARTOK ET. AL., GUIDE FOR CYBERSECURITY EVENT RECOVERY, NIST SPECIAL PUBLICATION 800-184 (2016), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf.

[213] NIST, *supra* note 165, at 19.

[214] *Id.* at 34–35.

[215] *Id.* at 35.

[216] *Id*.