LAW OFFICES
MARSHALL S. ZOLLA
A PROFESSIONAL CORPORATION
2029 CENTURY PARK EAST
SUITE 1020
LOS ANGELES, CALIFORNIA 90067-2911
TELEPHONE (310) 407-0770
FACSIMILE (310) 407-0776

MARSHALL S. ZOLLA*†‡
DEBORAH ELIZABETH ZOLLA
VIVIAN CARRASCO HOSP
*CERTIFIED SPECIALIST - FAMILY LAW
THE STATE BAR OF CALIFORNIA
BOARD OF LEGAL SPECIALIZATION
† A PROFESSIONAL CORPORATION
‡ FELLOW, AMERICAN ACADEMY OF
MATRIMONIAL LAWYERS
WWW.ZOLLALAW.COM

OF COUNSEL
JOEL P. SCHIFF*†
KEHR, SCHIFF & CRANE LLP
*CERTIFIED SPECIALIST - APPELLATE LAW
THE STATE BAR OF CALIFORNIA
BOARD OF LEGAL SPECIALIZATION
†ALSO ADMITTED IN THE STATE OF NEW YORK

FAMILY LAW SECTION
LOS ANGELES COUNTY BAR ASSOCIATION
2017 FAMILY LAW SYMPOSIUM
MAY 6, 2017

EVOLVING DUTIES OF FAMILY LAW ATTORNEYS RE INFORMATION TECHNOLOGY, ELECTRONIC EVIDENCE [ESI], AND CYBER SECURITY

I. CALIFORNIA ELECTRONIC DISCOVERY ACT [JUNE 29, 2009] [Amended 2012, effective June 1, 2013]

A. California modeled its electronic discovery act to conform with mostly parallel provisions in the 2006 Amendments to the Federal Rules of Civil Procedure.

1. Electronic discovery is covered in Code of Civil Procedure sections 1985.8, 2016.020[ESI], 2031.030, 2031.060, 2031.280, 2031.285, 2031.310, and 2031.320.

2. The scope of discovery is set forth in Code of Civil Procedure section 2031.010.

3. Mandated early meet and confer requirement is contained in California Rules of Court, Rule 3.724.

4. The form of production of ESI is referenced in Code of Civil Procedure sections 2031.030(a)(2) and 2031.280(c); 1985.8.

II. STATE BAR OF CALIFORNIA STANDING COMMITTEE ON PROFESSIONAL RESPONSIBILITY AND CONDUCT; ABA MODEL RULES OF PROFESSIONAL CONDUCT

A. State Bar Formal Opinion 2015-193: What are an attorney's ethical duties in the handling of discovery of electronically stored information? (attached hereto as Exhibit 1)

1. This important opinion interprets Rules 3-100 and 3-110 of the Rules of Professional Conduct of the State Bar of California, Business and Professions Code 6068e, and Evidence Code sections 952, 954, and 955.

B. State Bar Formal Opinion 2010-179: Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties? (attached hereto as Exhibit 2)

C. Electronic Ethics: Lawyers' Ethical Obligations in a Cyber Practice, Georgetown Journal of Legal Ethics, 29 GEO.J Legal Ethics 1237 (Fall, 2016). (attached hereto as Exhibit 3)

D. ABA Model Rules of Professional Conduct

1. ABA Model Rules of Professional Conduct 1.1: [An attorney] shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

2. ABA Model Rules of Professional Conduct 1.6(c): Attorneys have an affirmative duty to *make reasonable efforts* to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to information relating to the representation of a client.

3. Comment 8, ABA Model Rule 1.1: Competent representation is defined as "to maintain the requisite knowledge and skill, [an attorney] should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*."

4. Comment 6, ABA Model Rules of Professional Conduct 1.6(c): Attorneys have an affirmative duty to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

5. Cyber Security Consequences for the Law Firm and the Case: ABA Commission on Ethics Recommendations:

a. Provide adequate physical protection for devices for deleting data remotely in the event that a device is lost or stolen
b. Require the use of strong passwords
c. Purge data from devices before they are replaced
d. Install appropriate safeguards against malware or spyware
e. Ensure frequent backups of data

f. Update computer operating systems to ensure they contain the latest security protections

g. Configure software and network settings to minimize risk

h. Encrypt sensitive information and identify metadata from electronic documents before transmission

i. Avoid "wifi hotspots" in public places when transmitting confidential information

E. Attorneys Duties to Clients Regarding E-Discovery
[Material provided by Gordon D. Cruse, Esq.[1]]

1. Attorney has affirmative duty to explain discovery obligations to client, (see, Metro Opera Ass'n v. Local 100, Hotel Employees & Restaurant Employees Int'l Union (SDNY 2003) 212 FRD 178,222)

2. Duty of Preservation of ESI Runs First to Counsel

3. Duty to Advise Client of the Type of Information Potentially Relevant to the Suit and the Advise of the necessity Preventing its Destruction, (see, Green v. McClendon (SDNY 2009) 262 FRD 284)

4. Counsel Must Inform Itself About the Evidence in its Client's Possession and Adequately Counsel the Client Regarding the Kind of Records that are Responsive, (see, Tarlton v. Cumberland County Corr Fac (DNJ 2000) 192 FRD 165, 170)

5. Attorney has Duty to be Actively Involved in or Monitor E-Discovery Collections (see, Zubulake v. UBS Warberg LLC (SDNY 2004) 229 FRD 435)

6. Attorney must have Reasonable Understanding of Client's ESI and Computer Systems. (Tarlton)

7. Attorneys have Duty to Assist and Monitor Litigation Holds (see, Zubulake)

8. Attorney has Duty to Conduct Reasonable Investigation of Foundation for Electronic Discovery Responses & Representations, (See, 1100 West LLC v. Red Spot Paint (SD Ind 2009) 2009 US Dist Lexis 47439)

9. Attorney Bears Responsibility for Client Misconduct Known or Assisted by Counsel, (See, Qualcomm v. Broadcom 548 F.3d 1004 (2008)

10. Attorneys Must Meet and Confer in Good Faith on E-Discovery Issues, (see FRCP 26); California Rule of Court 3.724.

11. Negligence or Lack of Basic Knowledge Regarding E-discovery Requirements Constitutes Incompetence. (see, Zubulake)

III. CIVIL CODE SECTION 1798.82(b): A PERSON OR BUSINESS THAT SUFFERS A DATA BREACH MUST NOTIFY OWNERS OF THE DATA IMMEDIATELY FOLLOWING DISCOVERY OF THE UNAUTHORIZED ACCESS. [Copy of Statute Attached as Exhibit 4]

IV. CYBER SECURITY RISKS AND REQUIREMENTS

A. 2016 ABA Legal Technology Survey Report [Available at: https://www.americanbar.org/publications/techreport/2016/security.html]

1. Between 2% and 3% of overall firms that experienced a breach reported it led to unauthorized access to sensitive client data

2. Presence of Security Incident Response Policy:
   a. There are no respondents in firms of 500+ reporting none
   b. 2% of firms with 100-499 attorneys have none
   c. 4% of firms with 50-99 have none
   d. 5% with 10-49 have none
   e. 25% in firms with 2-9
   f. 41% of responding solos have none

3. "[Hackers] see attorneys as a backdoor to the valuable data of their corporate clients," - FBI Cyber Division

B. California Data Breach Report, California Department of Justice, February 2016 . [Selected Excerpt Attached Hereto as Exhibit 5]

V. **NEW E-FILING IN LOS ANGELES SUPERIOR COURT**

A. Judge Lewis has announced that the Family Law Department of the Los Angeles Superior Court will start E-Filing in September, 2017. Counsel will need to use approved electronic service providers. In this regard, several questions need to be addressed and clarified:

1. For confidential Court files and filing, such as paternity actions, what safeguards will be required to protect electronic transmission of such confidential documents?

2. If documents are ordered to be filed under seal, pursuant to California Rule of Court, Rules 2.550 and 2.551, what safeguards will be implemented to protect the confidentially of such electronic filings.

3. What Cyber security safeguards will the electronic service providers (vendors) be required to have in place?

4. Can the filing of documents be encrypted for security?

5. What is the procedure for conforming copies or proving that they were timely filed?

RESOURCES AND COMMENTS

A. Seminal Case Re Admissibility of Electronically Stored Information (Lorraine v. Markel American Insurance Company 241 F.R.D. 534 (2007).

B. *Vasquez v. California School of Culinary Arts, Inc.* (2014) 230 Cal.App.4th 35 [interpretation and application of Code of Civil Procedure section 1985.8 and Federal case law decisions regarding subpoenas, production of electronically stored information (ESI), and requirements for complying with a subpoena seeking ESI].

C. *In re Marriage of Evilsizor & Sweeney*, (2015) 237 Cal.App.4th 1416. [Husband downloaded wife's cell phone content, filed some downloaded text messages with the Court and disseminated them to third parties. Trial Court prohibited husband from distributing the information without permission of the Court. Affirmed on appeal. No prior restraint of husband's free speech, and husband's conduct held "abuse" under the DVPA].

EXHIBITS

1. State Bar Formal Opinion 2015-193: What are an attorney's ethical duties in the handling of discovery of electronically stored information?

2. State Bar Formal Opinion 2010-179: Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?

3. Electronic Ethics: Lawyers' Ethical Obligations in a Cyber Practice, Georgetown Journal of Legal Ethics, 29 GEO.J Legal Ethics 1237 (Fall, 2016).

4. Civil Code Section 1798.82(b)

5. California Data Breach Report, California Department of Justice, February 2016

FOOTNOTES

1. Gordon D. Cruse is the Co-Chair of the AAML's Practice & Technology Committee. Mr. Cruse is a graduate of the Georgetown Advanced ESI Institute. Gordon is a nationally recognized E-Discovery expert, consulting and teaching throughout the country.

Exhibit "1"

THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION NO. 2015-193

ISSUE: What are an attorney's ethical duties in the handling of discovery of electronically stored information?

DIGEST: An attorney's obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law. Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a matter, and the nature of the ESI. Competency may require even a highly experienced attorney to seek assistance in some litigation matters involving ESI. An attorney lacking the required competence for e-discovery issues has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation. Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney's duty of confidentiality.

AUTHORITIES INTERPRETED: Rules 3-100 and 3-110 of the Rules of Professional Conduct of the State Bar of California.[1/]

Business and Professions Code section 6068(e).

Evidence Code sections 952, 954 and 955.

STATEMENT OF FACTS

Attorney defends Client in litigation brought by Client's Chief Competitor in a judicial district that mandates consideration of e-discovery[2/] issues in its formal case management order, which is consistent with California Rules of Court, rule 3.728. Opposing Counsel demands e-discovery; Attorney refuses. They are unable to reach an agreement by the time of the initial case management conference. At that conference, an annoyed Judge informs both attorneys they have had ample prior notice that e-discovery would be addressed at the conference and tells them to return in two hours with a joint proposal.

In the ensuing meeting between the two lawyers, Opposing Counsel suggests a joint search of Client's network, using Opposing Counsel's chosen vendor, based upon a jointly agreed search term list. She offers a clawback agreement that would permit Client to claw back any inadvertently produced ESI that is protected by the attorney-client privilege and/or the work product doctrine ("Privileged ESI").

1/ Unless otherwise indicated, all references to rules in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

2/ Electronically stored information ("ESI") is information that is stored in technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities (e.g., Code Civ. Proc., § 2016.020, sub. (d) – (e)). Electronic Discovery, also known as e-discovery, is the use of legal means to obtain ESI in the course of litigation for evidentiary purposes.

Attorney believes the clawback agreement will allow him to pull back anything he "inadvertently" produces. Attorney concludes that Opposing Counsel's proposal is acceptable and, after advising Client about the terms and obtaining Client's authority, agrees to Opposing Counsel's proposal. Judge thereafter approves the attorneys' joint agreement and incorporates it into a Case Management Order, including the provision for the clawback of Privileged ESI. The Court sets a deadline three months later for the network search to occur.

Back in his office, Attorney prepares a list of keywords he thinks would be relevant to the case, and provides them to Opposing Counsel as Client's agreed upon search terms. Attorney reviews Opposing Counsel's additional proposed search terms, which on their face appear to be neutral and not advantageous to one party or the other, and agrees that they may be included.

Attorney has represented Client before, and knows Client is a large company with an information technology ("IT") department. Client's CEO tells Attorney there is no electronic information it has not already provided to Attorney in hard copy form. Attorney assumes that the IT department understands network searches better than he does and, relying on that assumption and the information provided by CEO, concludes it is unnecessary to do anything further beyond instructing Client to provide Vendor direct access to its network on the agreed upon search date. Attorney takes no further action to review the available data or to instruct Client or its IT staff about the search or discovery. As directed by Attorney, Client gives Vendor unsupervised direct access to its network to run the search using the search terms.

Subsequently, Attorney receives an electronic copy of the data retrieved by Vendor's search and, busy with other matters, saves it in an electronic file without review. He believes that the data will match the hard copy documents provided by Client that he already has reviewed, based on Client's CEO's representation that all information has already been provided to Attorney.

A few weeks later, Attorney receives a letter from Opposing Counsel accusing Client of destroying evidence and/or spoliation. Opposing Counsel threatens motions for monetary and evidentiary sanctions. After Attorney receives this letter, he unsuccessfully attempts to open his electronic copy of the data retrieved by Vendor's search. Attorney hires an e-discovery expert ("Expert"), who accesses the data, conducts a forensic search, and tells Attorney potentially responsive ESI has been routinely deleted from Client's computers as part of Client's normal document retention policy, resulting in gaps in the document production. Expert also advises Attorney that, due to the breadth of Vendor's execution of the jointly agreed search terms, both privileged information and irrelevant but highly proprietary information about Client's upcoming revolutionary product were provided to Chief Competitor in the data retrieval. Expert advises Attorney that an IT professional with litigation experience likely would have recognized the overbreadth of the search and prevented the retrieval of the proprietary information.

What ethical issues face Attorney relating to the e-discovery issues in this hypothetical?

DISCUSSION

I. Duty of Competence

A. Did Attorney Violate The Duty of Competence Arising From His Own Acts/Omissions?

While e-discovery may be relatively new to the legal profession, an attorney's core ethical duty of competence remains constant. Rule 3-110(A) provides: "A member shall not intentionally, recklessly, or repeatedly fail to perform legal services with competence." Under subdivision (B) of that rule, "competence" in legal services shall mean to apply the diligence, learning and skill, and mental, emotional, and physical ability reasonably necessary for the performance of such service. Read together, a mere failure to act competently does not trigger discipline under rule 3-110. Rather, it is the failure to do so in a manner that is intentional, reckless or repeated that would result in a disciplinable rule 3-110 violation. (See *In the Matter of Torres* (Reviwe Dept. 2000) 4 Cal. State Bar Ct. Rptr. 138, 149 ("We have repeatedly held that negligent legal representation, even that amounting to legal malpractice, does not establish a [competence] rule 3-110(A) violation."); see also, *In the Matter of Gadda* (Review Dept. 2002) 4 Cal. State Bar Ct. Rptr. 416 (reckless and repeated acts); *In the Matter of Riordan* (Review Dept. 2007) 5 Cal. State Bar Ct. Rptr. 41 (reckless and repeated acts).)

Legal rules and procedures, when placed alongside ever-changing technology, produce professional challenges that attorneys must meet to remain competent. Maintaining learning and skill consistent with an attorney's duty of competence includes keeping "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, . . ." ABA Model Rule 1.1, Comment [8].[3/] Rule 3-110(C) provides: "If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required." Another permissible choice would be to decline the representation. When e-discovery is at issue, association or consultation may be with a non-lawyer technical expert, if appropriate in the circumstances. Cal. State Bar Formal Opn. No. 2010-179.

Not every litigated case involves e-discovery. Yet, in today's technological world, almost every litigation matter *potentially* does. The chances are significant that a party or a witness has used email or other electronic communication, stores information digitally, and/or has other forms of ESI related to the dispute. The law governing e-discovery is still evolving. In 2009, the California Legislature passed California's Electronic Discovery Act adding or amending several California discovery statutes to make provisions for electronic discovery. See, e.g., Code of Civil Procedure section 2031.010, paragraph (a) (expressly providing for "copying, testing, or sampling" of "electronically stored information in the possession, custody, or control of any other party to the action.")[4/] However, there is little California case law interpreting the Electronic Discovery Act, and much of the development of e-discovery law continues to occur in the federal arena. Thus, to analyze a California attorney's current ethical obligations relating to e-discovery, we look to the federal jurisprudence for guidance, as well as applicable Model Rules, and apply those principles based upon California's ethical rules and existing discovery law.[5/]

We start with the premise that "competent" handling of e-discovery has many dimensions, depending upon the complexity of e-discovery in a particular case. The ethical duty of competence requires an attorney to assess at the outset of each case what electronic discovery issues might arise during the litigation, including the likelihood that e-discovery will or should be sought by either side. If e-discovery will probably be sought, the duty of competence requires an attorney to assess his or her own e-discovery skills and resources as part of the attorney's duty to provide the client with competent representation. If an attorney lacks such skills and/or resources, the attorney must try to acquire sufficient learning and skill, or associate or consult with someone with expertise to assist. Rule 3-110(C). Attorneys handling e-discovery should be able to perform (either by themselves or in association with competent co-counsel or expert consultants) the following:

- initially assess e-discovery needs and issues, if any;
- implement/cause to implement appropriate ESI preservation procedures;[6/]

[3/] Although not binding, opinions of ethics committees in California should be consulted by members for guidance on proper professional conduct. Ethics opinions and rules and standards promulgated by other jurisdictions and bar associations may also be considered. Rule 1-100(A).

[4/] In 2006, revisions were made to the Federal Rules of Civil Procedure, rules 16, 26, 33, 34, 37 and 45, to address e-discovery issues in federal litigation. California modeled its Electronic Discovery Act to conform with mostly-parallel provisions in those 2006 federal rules amendments. (See Evans, *Analysis of the Assembly Committee on Judiciary regarding AB 5* (2009). (http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab_0001-0050/ab_5_cfa_20090302_114942_asm_comm.html).)

[5/] Federal decisions are compelling where the California law is based upon a federal statute or the federal rules. (See *Toshiba America Electronic Components, Inc. v. Superior Court (Lexar Media, Inc.)* (2004) 124 Cal.App.4th 762, 770 [21 Cal.Rptr.3d 532]; *Vasquez v. Cal. School of Culinary Arts, Inc.* (2014) 230 Cal.App.4th 35 [178 Cal.Rptr.3d 10]; see also footnote 4, *supra.*)

[6/] This opinion does not directly address ethical obligations relating to litigation holds. A litigation hold is a directive issued to, by, or on behalf of a client to persons or entities associated with the client who may possess potentially relevant documents (including ESI) that directs those custodians to preserve such documents, pending further direction. See generally Redgrave, *Sedona Conference ® Commentary on Legal Holds: The Trigger and The Process* (Fall 2010) The Sedona Conference Journal, Vol. 11 at pp. 260 – 270, 277 – 279. Prompt issuance of a litigation hold may prevent spoliation of evidence, and the duty to do so falls on both the party and outside counsel working on the matter. See

- analyze and understand a client's ESI systems and storage;
- advise the client on available options for collection and preservation of ESI;
- identify custodians of potentially relevant ESI;
- engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan;
- perform data searches;
- collect responsive ESI in a manner that preserves the integrity of that ESI; and
- produce responsive non-privileged ESI in a recognized and appropriate manner.[7/]

See, e.g., *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC* (S.D.N.Y. 2010) 685 F.Supp.2d 456, 462 – 465 (defining gross negligence in the preservation of ESI), (abrogated on other grounds in *Chin v. Port Authority* (2nd Cir. 2012) 685 F.3d 135 (failure to institute litigation hold did not constitute gross negligence per se)).

In our hypothetical, Attorney had a general obligation to make an e-discovery evaluation early, prior to the initial case management conference. The fact that it was the standard practice of the judicial district in which the case was pending to address e-discovery issues in formal case management highlighted Attorney's obligation to conduct an early initial e-discovery evaluation.

Notwithstanding this obligation, Attorney made *no* assessment of the case's e-discovery needs or of his own capabilities. Attorney exacerbated the situation by not consulting with another attorney or an e-discovery expert prior to agreeing to an e-discovery plan at the initial case management conference. He then allowed that proposal to become a court order, again with no expert consultation, although he lacked sufficient expertise. Attorney participated in preparing joint e-discovery search terms without experience or expert consultation, and he did not fully understand the danger of overbreadth in the agreed upon search terms.

Even after Attorney stipulated to a court order directing a search of Client's network, Attorney took no action other than to instruct Client to allow Vendor to have access to Client's network. Attorney did not instruct or supervise Client regarding the direct network search or discovery, nor did he try to pre-test the agreed upon search terms or otherwise review the data before the network search, relying on his assumption that Client's IT department would know what to do, and on the parties' clawback agreement.

After the search, busy with other matters and under the impression the data matched the hard copy documents he had already seen, Attorney took no action to review the gathered data until after Opposing Counsel asserted spoliation and threatened sanctions. Attorney then unsuccessfully attempted to review the search results. It was only then, at the end of this long line of events, that Attorney finally consulted an e-discovery expert and learned of the e-discovery problems facing Client. By this point, the potential prejudice facing Client was significant, and much of the damage already had been done.

At the least, Attorney risked breaching his duty of competence when he failed at the outset of the case to perform a timely e-discovery evaluation. Once Opposing Counsel insisted on the exchange of e-discovery, it became certain that e-discovery would be implicated, and the risk of a breach of the duty of competence grew considerably; this should have prompted Attorney to take additional steps to obtain competence, as contemplated under rule 3-110(C), such as consulting an e-discovery expert.

[Footnote Continued...]

Zubulake v. UBS Warburg LLC (S.D.N.Y. 2003) 220 F.R.D. 212, 218 and *Zubulake v. UBS Warburg LLC* (S.D.N.Y. 2004) 229 F.R.D. 422, 432. Spoliation of evidence can result in significant sanctions, including monetary and/or evidentiary sanctions, which may impact a client's case significantly.

[7/] This opinion focuses on an attorney's ethical obligations relating to his own client's ESI and, therefore, this list focuses on those issues. This opinion does not address the scope of an attorney's duty of competence relating to obtaining an opposing party's ESI.

Had the e-discovery expert been consulted at the beginning, or at the latest once Attorney realized e-discovery would be required, the expert could have taken various steps to protect Client's interest, including possibly helping to structure the search differently, or drafting search terms less likely to turn over privileged and/or irrelevant but highly proprietary material. An expert also could have assisted Attorney in his duty to counsel Client of the significant risks in allowing a third party unsupervised direct access to Client's system due to the high risks and how to mitigate those risks. An expert also could have supervised the data collection by Vendor.[8/]

Whether Attorney's acts/omissions in this single case amount to a disciplinable offense under the "intentionally, recklessly, or repeatedly" standard of rule 3-110 is beyond this opinion, yet such a finding could be implicated by these facts.[9/] See, e.g., *In the Matter of Respondent G.* (Review Dept. 1992) 2 Cal. State Bar Ct. Rptr. 175, 179 (respondent did not perform competently where he was reminded on repeated occasions of inheritance taxes owed and repeatedly failed to advise his clients of them); *In re Matter of Copren* (Review Dept. 2005) 4 Cal. State Bar Ct. Rptr. 861, 864 (respondent did not perform competently when he failed to take several acts in single bankruptcy matter); *In re Matter of Layton* (Review Dept. 1993) 2 Cal. State Bar Ct. Rptr. 366, 377 – 378 (respondent did not perform competently where he "recklessly" exceeded time to administer estate, failed to diligently sell/distribute real property, untimely settled supplemental accounting and did not notify beneficiaries of intentions not to sell/lease property).

B. Did Attorney Violate The Duty of Competence By Failing To Supervise?

The duty of competence in rule 3-110 includes the duty to supervise the work of subordinate attorneys and non-attorney employees or agents. See Discussion to rule 3-110. This duty to supervise can extend to outside vendors or contractors, and even to the client itself. See California State Bar Formal Opn. No. 2004-165 (duty to supervise outside contract lawyers); San Diego County Bar Association Formal Opn. No. 2012-1 (duty to supervise clients relating to ESI, citing *Cardenas v. Dorel Juvenile Group, Inc.* (D. Kan. 2006) 2006 WL 1537394).

Rule 3-110(C) permits an attorney to meet the duty of competence through association with another lawyer or consultation with an expert. See California State Bar Formal Opn. No. 2010-179. Such expert may be an outside vendor, a subordinate attorney, or even the client, if they possess the necessary expertise. This consultation or association, however, does not absolve an attorney's obligation to supervise the work of the expert under rule 3-110, which is a non-delegable duty belonging to the attorney who is counsel in the litigation, and who remains the one primarily answerable to the court. An attorney must maintain overall responsibility for the work of the expert he or she chooses, even if that expert is the client or someone employed by the client. The attorney must do so by remaining regularly engaged in the expert's work, by educating everyone involved in the e-discovery workup about the legal issues in the case, the factual matters impacting discovery, including witnesses and key evidentiary issues, the obligations around discovery imposed by the law or by the court, and of any relevant risks associated with the e-discovery tasks at hand. The attorney should issue appropriate instructions and guidance and, ultimately, conduct appropriate tests until satisfied that the attorney is meeting his ethical obligations prior to releasing ESI.

Here, relying on his familiarity with Client's IT department, Attorney assumed the department understood network searches better than he did. He gave them no further instructions other than to allow Vendor access on the date of the network search. He provided them with no information regarding how discovery works in litigation, differences

---

[8/] See Advisory Committee Notes to the 2006 Amendments to the Federal Rules of Civil Procedure, rule 34 ("Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) . . . is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems."). See also The Sedona Principles Addressing Electronic Document Production (2nd Ed. 2007), Comment 10(b) ("Special issues may arise with any request to secure direct access to electronically stored information or to computer devices or systems on which it resides. Protective orders should be in place to guard against any release of proprietary, confidential, or personal electronically stored information accessible to the adversary or its expert.").

[9/] This opinion does not intend to set or define a standard of care of attorneys for liability purposes, as standards of care can be highly dependent on the factual scenario and other factors not applicable to our analysis herein.

between a party affiliated vendor and a neutral vendor, what could constitute waiver under the law, what case-specific issues were involved, or the applicable search terms. Client allowed Vendor direct access to its entire network, without the presence of any Client representative to observe or monitor Vendor's actions. Vendor retrieved proprietary trade secret and privileged information, a result Expert advised Attorney could have been prevented had a trained IT individual been involved from the outset. In addition, Attorney failed to warn Client of the potential significant legal effect of not suspending its routine document deletion protocol under its document retention program.

Here, as with Attorney's own actions/inactions, whether Attorney's reliance on Client was reasonable and sufficient to satisfy the duty to supervise in this setting is a question for a trier of fact. Again, however, a potential finding of a competence violation is implicated by the fact pattern. See, e.g., *Palomo v. State Bar* (1984) 36 Cal.3d 785, 796 [205 Cal.Rptr. 834] (evidence demonstrated lawyer's pervasive carelessness in failing to give the office manager any supervision, or instruction on trust account requirements and procedures).

II. Duty of Confidentiality

A fundamental duty of an attorney is "[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client." (Bus. & Prof. Code, § 6068 (e)(1).) "Secrets" includes "information, other than that protected by the attorney-client privilege, that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client." (Cal. State Bar Formal Opinion No. 1988-96.) "A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1), without the informed consent of the client, or as provided in paragraph (B) of this rule." (Rule 3-100(A).)

Similarly, an attorney has a duty to assert the attorney-client privilege to protect confidential communications between the attorney and client. (Evid. Code, §§ 952, 954, 955.) In civil discovery, the attorney-client privilege will protect confidential communications between the attorney and client in cases of inadvertent disclosure *only if* the attorney and client act reasonably to protect that privilege. See *Regents of University of California v. Superior Court (Aquila Merchant Services, Inc.)* (2008) 165 Cal.App.4th 672, 683 [81 Cal.Rptr.3d 186]. This approach also echoes federal law. [10/] A lack of reasonable care to protect against disclosing privileged and protected information when producing ESI can be deemed a waiver of the attorney-client privilege. See *Kilopass Tech. Inc. v. Sidense Corp.* (N.D. Cal. 2012) 2012 WL 1534065 at 2 – 3 (attorney-client privilege deemed waived as to privileged documents released through e-discovery because screening procedures employed were unreasonable).

In our hypothetical, because of the actions taken by Attorney prior to consulting with any e-discovery expert, Client's privileged information has been disclosed. Due to Attorney's actions, Chief Competitor can argue that such disclosures were not "inadvertent" and that any privileges were waived. Further, non-privileged, but highly confidential proprietary information about Client's upcoming revolutionary new product has been released into the hands of Chief Competitor. Even absent any indication that Opposing Counsel did anything to engineer the overbroad disclosure, it remains true that the disclosure occurred because Attorney participated in creating overbroad search terms. All of this happened unbeknownst to Attorney, and only came to light after Chief Competitor accused Client of evidence spoliation. Absent Chief Competitor's accusation, it is not clear when any of this would have come to Attorney's attention, if ever.

The clawback agreement on which Attorney heavily relied may not work to retrieve the information from the other side. By its terms, the clawback agreement was limited to inadvertently produced Privileged ESI. Both privileged information, and non-privileged, but confidential and proprietary information, have been released to Chief Competitor.

[10/] See Federal Rules of Evidence, rule 502(b): "Inadvertent Disclosure. When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if: (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B)."

Under these facts, Client may have to litigate whether Client (through Attorney) acted diligently enough to protect its attorney-client privileged communications. Attorney took no action to review Client's network prior to allowing the network search, did not instruct or supervise Client prior to or during Vendor's search, participated in drafting the overbroad search terms, and waited until after Client was accused of evidence spoliation before reviewing the data – all of which could permit Opposing Counsel viably to argue Client failed to exercise due care to protect the privilege, and the disclosure was not inadvertent.[11/]

Client also may have to litigate its right to the return of non-privileged but confidential proprietary information, which was not addressed in the clawback agreement.

Whether a waiver has occurred under these circumstances, and what Client's rights are to return of its non-privileged/confidential proprietary information, again are legal questions beyond this opinion. Attorney did not reasonably try to minimize the risks. Even if Client can retrieve the information, Client may never "un-ring the bell."

The State Bar Court Review Department has stated, "Section 6068, subdivision (e) is the most strongly worded duty binding on a California attorney. It requires the attorney to maintain 'inviolate' the confidence and 'at every peril to himself or herself' preserve the client's secrets." (See *Matter of Johnson* (Rev. Dept. 2000) 4 Cal. State Bar Ct. Rptr. 179.) While the law does not require perfection by attorneys in acting to protect privileged or confidential information, it requires the exercise of reasonable care. Cal. State Bar Formal Opn. No. 2010-179. Here, Attorney took only minimal steps to protect Client's ESI, or to instruct/supervise Client in the gathering and production of that ESI, and instead released everything without prior review, inappropriately relying on a clawback agreement. Client's secrets are now in Chief Competitor's hands, and further, Chief Competitor may claim that Client has waived the attorney-client privilege. Client has been exposed to that potential dispute as the direct result of Attorney's actions. Attorney may have breached his duty of confidentiality to Client.

CONCLUSION

Electronic document creation and/or storage, and electronic communications, have become commonplace in modern life, and discovery of ESI is now a frequent part of almost any litigated matter. Attorneys who handle litigation may not ignore the requirements and obligations of electronic discovery. Depending on the factual circumstances, a lack of technological knowledge in handling e-discovery may render an attorney ethically incompetent to handle certain litigation matters involving e-discovery, absent curative assistance under rule 3-110(C), even where the attorney may otherwise be highly experienced. It also may result in violations of the duty of confidentiality, notwithstanding a lack of bad faith conduct.

This opinion is issued by the Standing Committee on Professional Responsibility and Conduct of the State Bar of California. It is advisory only. It is not binding upon the courts, the State Bar of California, its Board of Trustees, any persons or tribunals charged with regulatory responsibilities, or any member of the State Bar.

*[**Publisher's Note**: Internet resources cited in this opinion were last accessed by staff on June 30, 2015. Copies of these resources are on file with the State Bar's Office of Professional Competence.]*

[11/] Although statute, rules, and/or case law provide some limited authority for the legal claw back of certain inadvertently produced materials, even in the absence of an express agreement, those provisions may not work to mitigate the damage caused by the production in this hypothetical. These "default" claw back provisions typically only apply to privilege and work product information, and require both that the disclosure at issue has been truly inadvertent, and that the holder of the privilege has taken reasonable steps to prevent disclosure in the first instance. See Federal Rules of Evidence, rule 502; see also generally *State Compensation Insurance Fund v. WPS, Inc.* (1999) 70 Cal.App.4th 644 [82 Cal.Rptr.2d 799]; *Rico v. Mitsubishi Motors Corp.* (2007) 42 Cal.4th 807, 817 – 818 [68 Cal.Rptr.3d 758]. As noted above, whether the disclosures at issue in our hypothetical truly were "inadvertent" under either the parties' agreement or the relevant law is an open question. Indeed, Attorney will find even less assistance from California's discovery clawback statute than he will from the federal equivalent, as the California statute merely addresses the procedure for litigating a dispute on a claim of inadvertent production, and not the legal issue of waiver at all. (See Code Civ. Proc., § 2031.285.)

Exhibit "2"

THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION NO. 2010-179

ISSUE: Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?

DIGEST: Whether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications.

AUTHORITIES INTERPRETED: Rules 3-100 and 3-110 of the California Rules of Professional Conduct.

Business and Professions Code section 6068, subdivision (e)(1).

Evidence Code sections 917(a) and 952.

STATEMENT OF FACTS

Attorney is an associate at a law firm that provides a laptop computer for his use on client and firm matters and which includes software necessary to his practice. As the firm informed Attorney when it hired him, the computer is subject to the law firm's access as a matter of course for routine maintenance and also for monitoring to ensure that the computer and software are not used in violation of the law firm's computer and Internet-use policy. Unauthorized access by employees or unauthorized use of the data obtained during the course of such maintenance or monitoring is expressly prohibited. Attorney's supervisor is also permitted access to Attorney's computer to review the substance of his work and related communications.

Client has asked for Attorney's advice on a matter. Attorney takes his laptop computer to the local coffee shop and accesses a public wireless Internet connection to conduct legal research on the matter and email Client. He also takes the laptop computer home to conduct the research and email Client from his personal wireless system.

DISCUSSION

Due to the ever-evolving nature of technology and its integration in virtually every aspect of our daily lives, attorneys are faced with an ongoing responsibility of evaluating the level of security of technology that has increasingly become an indispensable tool in the practice of law. The Committee's own research – including conferring with computer security experts – causes it to understand that, without appropriate safeguards (such as firewalls, secure username/password combinations, and encryption), data transmitted wirelessly can be intercepted and read with increasing ease. Unfortunately, guidance to attorneys in this area has not kept pace with technology. Rather than engage in a technology-by-technology analysis, which would likely become obsolete shortly, this

opinion sets forth the general analysis that an attorney should undertake when considering use of a particular form of technology.

1. The Duty of Confidentiality

In California, attorneys have an express duty "[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client."[1/] (Bus. & Prof. Code, § 6068, subd. (e)(1).) This duty arises from the relationship of trust between an attorney and a client and, absent the informed consent of the client to reveal such information, the duty of confidentiality has very few exceptions. (Rules Prof. Conduct, rule 3-100 & discussion ["[A] member may not reveal such information except with the consent of the client or as authorized or required by the State Bar Act, these rules, or other law."].)[2/]

Unlike Rule 1.6 of the Model Rules of Professional Conduct ("MRPC"), the exceptions to the duty of confidentiality under rule 3-100 do not expressly include disclosure "impliedly authorized in order to carry out the representation." (MRPC, Rule 1.6.) Nevertheless, the absence of such language in the California Rules of Professional Conduct does not prohibit an attorney from using postal or courier services, telephone lines, or other modes of communication beyond face-to-face meetings, in order to effectively carry out the representation. There is a distinction between actually disclosing confidential information to a third party for purposes ancillary to the representation,[3/] on the one hand, and using appropriately secure technology provided by a third party as a method of communicating with the client or researching a client's matter,[4/] on the other hand.

Section 952 of the California Evidence Code, defining "confidential communication between client and lawyer" for purposes of application of the attorney-client privilege, includes disclosure of information to third persons "to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted." (Evid. Code, § 952.) While the duty to protect confidential client information is broader in scope than the attorney-client privilege (Discussion [2] to rule 3-100; *Goldstein v. Lees* (1975) 46 Cal.App.3d 614, 621, fn. 5 [120 Cal.Rptr. 253]), the underlying principle remains the same, namely, that transmission of information through a third party reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information. (See Cal. State Bar Formal Opn. No. 2003-161 [repeating the Committee's prior observation "that the duty of confidentiality and the evidentiary privilege share the same basic policy foundation: to encourage clients to disclose all possibly pertinent information to their attorneys so that the attorneys may effectively represent the clients' interests."].) Pertinent here, the manner in which an attorney acts to safeguard confidential client information is governed by the duty of competence, and determining whether a third party has the ability to access and use confidential client information in a manner that is unauthorized by the client is a subject that must be considered in conjunction with that duty.

2. The Duty of Competence

Rule 3-110(A) prohibits the intentional, reckless or repeated failure to perform legal services with competence. Pertinent here, "competence" may apply to an attorney's diligence and learning with respect to handling matters for clients. (Rules Prof. Conduct, rule 3-110(B).) The duty of competence also applies to an attorney's "duty to supervise the work of subordinate attorney and non-attorney employees or agents." (Discussion to rule 3-110.)

1/ "Secrets" include "[a]ny 'information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would likely be detrimental to the client.'" (Cal. State Bar Formal Opn. No. 1981-58.)

2/ Unless otherwise indicated, all future references to rules in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

3/ In this regard, compare Cal. State Bar Formal Opn. No. 1971-25 (use of an outside data processing center without the client's consent for bookkeeping, billing, accounting and statistical purposes, if such information includes client secrets and confidences, would violate section 6068, subdivision (e)), with Los Angeles County Bar Assn. Formal Opn. No. 374 (1978) (concluding that in most circumstances, if protective conditions are observed, disclosure of client's secrets and confidences to a central data processor would not violate section 6068(e) and would be the same as disclosures to non-lawyer office employees).

4/ Cf. Evid. Code, § 917(b) ("A communication ... does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.").

With respect to acting competently to preserve confidential client information, the comments to Rule 1.6 of the MRPC[5] provide:

> [16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.
>
> [17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

(MRPC, cmts. 16 & 17 to Rule 1.6.) In this regard, the duty of competence includes taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential and that the attorney's handling of such information does not result in a waiver of any privileges or protections.

3. Factors to Consider

In accordance with the duties of confidentiality and competence, an attorney should consider the following before using a specific technology:[6]

a) The attorney's ability to assess the level of security afforded by the technology, including without limitation:

   i) Consideration of how the particular technology differs from other media use. For example, while one court has stated that, "[u]nlike postal mail, simple e-mail generally is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)" (*American Civil Liberties Union v. Reno* (E.D.Pa. 1996) 929 F.Supp. 824, 834, aff'd (1997) 521 U.S. 844 [117 S.Ct. 2329]), most bar associations have taken the position that the risks of a third party's unauthorized review of email (whether by interception or delivery to an unintended recipient) are similar to the risks that confidential client information transmitted by standard mail service will be opened by any of the many hands it passes through on the way to its recipient or will be misdirected[7] (see, e.g., ABA Formal Opn. No. 99-413[8] [concluding that attorneys have a reasonable expectation of privacy in email communications, even if unencrypted, "despite some risk of interception and disclosure"]; Los Angeles County Bar Assn. Formal Opn. No. 514 (2005) ["Lawyers are not required

---

[5] In the absence of on-point California authority and conflicting state public policy, the MRPC may serve as guidelines. (*City & County of San Francisco v. Cobra Solutions, Inc.* (2006) 38 Cal. 4th 839, 852 [43 Cal.Rptr.3d 771].)

[6] These factors should be considered regardless of whether the attorney practices in a law firm, a governmental agency, a non-profit organization, a company, as a sole practitioner or otherwise.

[7] Rule 1-100(A) provides that "[e]thics opinions and rules and standards promulgated by other jurisdictions and bar associations may . . . be considered" for professional conduct guidance.

[8] In 1999, the ABA Committee on Ethics and Professional Responsibility reviewed state bar ethics opinions across the country and determined that, as attorneys' understanding of technology has improved, the opinions generally have transitioned from concluding that use of Internet email violates confidentiality obligations to concluding that use of unencrypted Internet email is permitted without express client consent. (ABA Formal Opn. No. 99-413 [detailing various positions taken in state ethics opinions from Alaska, Washington D.C., Kentucky, New York, Illinois, North Dakota, South Carolina, Vermont, Pennsylvania, Arizona, Iowa and North Carolina].)

to encrypt e-mail containing confidential client communications because e-mail poses no greater risk of interception and disclosure than regular mail, phones or faxes."]; Orange County Bar Assn. Formal Opn. No. 97-0002 [concluding use of encrypted email is encouraged, but not required].) (See also *City of Reno v. Reno Police Protective Assn.* (2003) 118 Nev. 889, 897-898 [59 P.3d 1212] [referencing an earlier version of section 952 of the California Evidence Code and concluding "that a document transmitted by e-mail is protected by the attorney-client privilege as long as the requirements of the privilege are met."].)

ii) Whether reasonable precautions may be taken when using the technology to increase the level of security.[9/] As with the above-referenced views expressed on email, the fact that opinions differ on whether a particular technology is secure suggests that attorneys should take reasonable steps as a precautionary measure to protect against disclosure.[10/] For example, depositing confidential client mail in a secure postal box or handing it directly to the postal carrier or courier is a reasonable step for an attorney to take to protect the confidentiality of such mail, as opposed to leaving the mail unattended in an open basket outside of the office door for pick up by the postal service. Similarly, encrypting email may be a reasonable step for an attorney to take in an effort to ensure the confidentiality of such communications remain so when the circumstance calls for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous. To place the risks in perspective, it should not be overlooked that the very nature of digital technologies makes it easier for a third party to intercept a much greater amount of confidential information in a much shorter period of time than would be required to transfer the same amount of data in hard copy format. In this regard, if an attorney can readily employ encryption when using public wireless connections and has enabled his or her personal firewall, the risks of unauthorized access may be significantly reduced.[11/] Both of these tools are readily available and relatively inexpensive, and may already be built into the operating system. Likewise, activating password protection features on mobile devices, such as laptops and PDAs, presently helps protect against access to confidential client information by a third party if the device is lost, stolen or left unattended. (See David Ries & Reid Trautz, *Law Practice Today*, "Securing Your Clients' Data While On the Road," October 2008 [noting reports that "as many as 10% of laptops used by American businesses are stolen during their useful lives and 97% of them are never recovered"].)

iii) Limitations on who is permitted to monitor the use of the technology, to what extent and on what grounds. For example, if a license to use certain software or a technology service imposes a requirement of third party access to information related to the attorney's use of the technology, the attorney may need to confirm that the terms of the requirement or authorization do not permit the third party to disclose confidential client information to others or use such information for any purpose other than to ensure the functionality of the software or that the technology is not being used for an improper purpose, particularly if the information at issue is highly sensitive.[12/] "Under Rule 5.3 [of the MRPC], a lawyer retaining such an outside service provider is required to make reasonable efforts to ensure that

---

[9/] Attorneys also should employ precautions to protect confidential information when in public, such as ensuring that the person sitting in the adjacent seat on an airplane cannot see the computer screen or moving to a private location before discussing confidential information on a mobile phone.

[10/] Section 60(1)(b) of the Restatement (Third) of The Law Governing Lawyers provides that "a lawyer must take steps reasonable in the circumstances to protect confidential client information against impermissible use or disclosure by the lawyer's associates or agents that may adversely affect a material interest of the client or otherwise than as instructed by the client."

[11/] Similarly, this Committee has stated that if an attorney is going to maintain client documents in electronic form, he or she must take reasonable steps to strip any metadata containing confidential information of other clients before turning such materials over to a current or former client or his or her new attorney. (See Cal. State Bar Formal Opn. 2007-174.)

[12/] A similar approach might be appropriate if the attorney is employed by a non-profit or governmental organization where information may be monitored by a person or entity with interests potentially or actually in conflict with the attorney's client. In such cases, the attorney should not use the technology for the representation, absent informed consent by the client or the ability to employ safeguards to prevent access to confidential client information. The attorney also may need to consider whether he or she can competently represent the client without the technology.

the service provider will not make unauthorized disclosures of client information. Thus when a lawyer considers entering into a relationship with such a service provider he must ensure that the service provider has in place, or will establish, reasonable procedures to protect the confidentiality of information to which it gains access, and moreover, that it fully understands its obligations in this regard. [Citation.] In connection with this inquiry, a lawyer might be well-advised to secure from the service provider in writing, along with or apart from any written contract for services that might exist, a written statement of the service provider's assurance of confidentiality." (ABA Formal Opn. No. 95-398.)

Many attorneys, as with a large contingent of the general public, do not possess much, if any, technological savvy. Although the Committee does not believe that attorneys must develop a mastery of the security features and deficiencies of each technology available, the duties of confidentiality and competence that attorneys owe to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.[13/] (Cf. Rules Prof. Conduct, rule 3-110(C) ["If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required."].)

b) Legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person's electronic information. The fact that a third party could be subject to criminal charges or civil claims for intercepting, accessing or engaging in unauthorized use of confidential client information favors an expectation of privacy with respect to a particular technology. (See, e.g., 18 U.S.C. § 2510 et seq. [Electronic Communications Privacy Act of 1986]; 18 U.S.C. § 1030 et seq. [Computer Fraud and Abuse Act]; Pen. Code, § 502(c) [making certain unauthorized access to computers, computer systems and computer data a criminal offense]; Cal. Pen. Code, § 629.86 [providing a civil cause of action to "[a]ny person whose wire, electronic pager, or electronic cellular telephone communication is intercepted, disclosed, or used in violation of [Chapter 1.4 on Interception of Wire, Electronic Digital Pager, or Electronic Cellular Telephone Communications]."]; *eBay, Inc. v. Bidder's Edge, Inc.* (N.D.Cal. 2000) 100 F.Supp.2d 1058, 1070 [in case involving use of web crawlers that exceeded plaintiff's consent, court stated "[c]onduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another's personal property, is sufficient to establish a cause of action for trespass to chattel."].)[14/]

c) The degree of sensitivity of the information. The greater the sensitivity of the information, the less risk an attorney should take with technology. If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent.[15/] As noted above, if another person may have access to the communications transmitted between the attorney and the client (or others necessary to the representation), and may have an interest in the information being disclosed that is in conflict with the client's interest, the attorney should take precautions to ensure that the person will not be able to access the information or should avoid using the technology. These types of situations increase the likelihood for intrusion.

[13/] Some potential security issues may be more apparent than others. For example, users of unsecured public wireless connections may receive a warning when accessing the connection. However, in most instances, users must take affirmative steps to determine whether the technology is secure.

[14/] Attorneys also have corresponding legal and ethical obligations not to invade the confidential and privileged information of others.

[15/] For the client's consent to be informed, the attorney should fully advise the client about the nature of the information to be transmitted with the technology, the purpose of the transmission and use of the information, the benefits and detriments that may result from transmission (both legal and nonlegal), and any other facts that may be important to the client's decision. (Los Angeles County Bar Assn. Formal Opn. No. 456 (1989).) It is particularly important for an attorney to discuss the risks and potential harmful consequences of using the technology when seeking informed consent.

d) Possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product, including possible waiver of the privileges.[16] Section 917(a) of the California Evidence Code provides that "a communication made in confidence in the course of the lawyer-client, physician-patient, psychotherapist-patient, clergy-penitent, husband-wife, sexual assault counselor-victim, or domestic violence counselor-victim relationship ... is presumed to have been made in confidence and the opponent of the claim of privilege has the burden of proof to establish that the communication was not confidential." (Evid. Code, § 917(a).) Significantly, subsection (b) of section 917 states that such a communication "does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication." (Evid. Code, § 917(b). See also Penal Code, § 629.80 ["No otherwise privileged communication intercepted in accordance with, or in violation of, the provisions of [Chapter 1.4] shall lose its privileged character."]; 18 U.S.C. § 2517(4) ["No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of [18 U.S.C. § 2510 et seq.] shall lose its privileged character."].) While these provisions seem to provide a certain level of comfort in using technology for such communications, they are not a complete safeguard. For example, it is possible that, if a particular technology lacks essential security features, use of such a technology could be deemed to have waived these protections. Where the attorney-client privilege is at issue, failure to use sufficient precautions may be considered in determining waiver.[17] Further, the analysis differs with regard to an attorney's duty of confidentiality. Harm from waiver of attorney-client privilege is possible depending on if and how the information is used, but harm from disclosure of confidential client information may be immediate as it does not necessarily depend on use or admissibility of the information, including as it does matters which would be embarrassing or would likely be detrimental to the client if disclosed.

e) The urgency of the situation. If use of the technology is necessary to address an imminent situation or exigent circumstances and other alternatives are not reasonably available, it may be reasonable in limited cases for the attorney to do so without taking additional precautions.

f) Client instructions and circumstances. If a client has instructed an attorney not to use certain technology due to confidentiality or other concerns or an attorney is aware that others have access to the client's electronic devices or accounts and may intercept or be exposed to confidential client information, then such technology should not be used in the course of the representation.[18]

4. Application to Fact Pattern[19]

In applying these factors to Attorney's situation, the Committee does not believe that Attorney would violate his duties of confidentiality or competence to Client by using the laptop computer because access is limited to authorized individuals to perform required tasks. However, Attorney should confirm that personnel have been appropriately instructed regarding client confidentiality and are supervised in accordance with rule 3-110. (See *Crane v. State Bar* (1981) 30 Cal.3d 117, 123 [177 Cal.Rptr. 670] ["An attorney is responsible for the work product of his employees which is performed pursuant to his direction and authority."]; *In re Complex Asbestos Litig.* (1991) 232 Cal.App.3d 572, 588 [283 Cal.Rptr. 732] [discussing law firm's ability to supervise employees and ensure they protect client confidences]; Cal. State Bar Formal Opn. No. 1979-50 [discussing lawyer's duty to explain to

---

[16] Consideration of evidentiary issues is beyond the scope of this opinion, which addresses only the ethical implications of using certain technologies.

[17] For example, with respect to the impact of inadvertent disclosure on the attorney-client privilege or work-product protection, rule 502(b) of the Federal Rules of Evidence states: "When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if: 1. the disclosure is inadvertent; 2. the holder of the privilege or protection took reasonable steps to prevent disclosure; and 3. the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B)." As a practical matter, attorneys also should use appropriate confidentiality labels and notices when transmitting confidential or privileged client information.

[18] In certain circumstances, it may be appropriate to obtain a client's informed consent to the use of a particular technology.

[19] In this opinion, we are applying the factors to the use of computers and wireless connections to assist the reader in understanding how such factors function in practice. Use of other electronic devices would require similar considerations.

employee what obligations exist with respect to confidentiality].) In addition, access to the laptop by Attorney's supervisor would be appropriate in light of her duty to supervise Attorney in accordance with rule 3-110 and her own fiduciary duty to Client to keep such information confidential.

With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall.[20/] Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.[21/]

Finally, if Attorney's personal wireless system has been configured with appropriate security features,[22/] the Committee does not believe that Attorney would violate his duties of confidentiality and competence by working on Client's matter at home. Otherwise, Attorney may need to notify Client of the risks and seek her informed consent, as with the public wireless connection.

CONCLUSION

An attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representation does not subject confidential client information to an undue risk of unauthorized disclosure. Because of the evolving nature of technology and differences in security features that are available, the attorney must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps.

This opinion is issued by the Standing Committee on Professional Responsibility and Conduct of the State Bar of California. It is advisory only. It is not binding upon the courts, the State Bar of California, its Board of Governors, any persons, or tribunals charged with regulatory responsibilities, or any member of the State Bar.

[20/] Local security features available for use on individual computers include operating system firewalls, antivirus and antispam software, secure username and password combinations, and file permissions, while network safeguards that may be employed include network firewalls, network access controls such as virtual private networks (VPNs), inspection and monitoring. This list is not intended to be exhaustive.

[21/] Due to the possibility that files contained on a computer may be accessed by hackers while the computer is operating on an unsecure network connection and when appropriate local security features, such as firewalls, are not enabled, attorneys should be aware that *any* client's confidential information stored on the computer may be at risk regardless of whether the attorney has the file open at the time.

[22/] Security features available on wireless access points will vary and should be evaluated on an individual basis.

Exhibit "3"

29 Geo. J. Legal Ethics 1237

Georgetown Journal of Legal Ethics
Fall, 2016

Current Development 2015-2016

ELECTRONIC ETHICS: LAWYERS' ETHICAL OBLIGATIONS IN A CYBER PRACTICE

Nathan Powell [a1]

INTRODUCTION

Information has become one of the most valuable commodities in our economy. With its increased value, and with our ever-increasing reliance on information technology (IT) systems, attempts to appropriate information for underhanded means have proportionately increased. Cybercrime has thus become one of the biggest threats to entities that manage large amounts of business and personal data. By 2016 we saw the hacking of major corporate and government entities such as Target, Home Depot, Sony Pictures Entertainment, and the Office of Personnel Management. Moreover, the average annual cost of cybercrime in 2015 for large U.S. companies was $15.4 million, up nineteen percent from the previous year and eighty-two percent from 2009. [1]

In this environment, cyber threats to law firms are also rapidly mounting. [2] Law enforcement agencies, such as the FBI and the U.S. Secret Service, have warned law firms that they are targets for thieves in China and Russia, seeking to capitalize on corporate secrets. [3] "Hacktivists," such as the group Anonymous, have infiltrated law firm networks with political goals. [4] Threats may also come ***1238** from malicious insiders and domestic organized crime. In 2010, the *National Law Journal* reported that the security consulting firm Mandiant had aided over 50 law firms after cybersecurity breaches. [5] In 2012, Mandiant published a report estimating that 80 percent of the 100 largest American law firms had some malicious computer breach in 2011. [6]

Law firms are attractive targets for attacks for several reasons. First, law firms, especially large law firms, are repositories for large amounts of highly valuable corporate data, including intellectual property, investment plans, trade secrets, and clients' business and litigation strategies. [7] According to the FBI, "[l]aw firms have a tremendous concentration of really critical, private information," which both state and non-state actors may desire to steal in order to gain advantages in the marketplace or in court. [8] Moreover, law firms represent more efficient targets than the clients they serve. Law firms "are usually involved in only their client's most important business matters, meaning hackers may not need to sift through extraneous data to find the more valuable information." [9]

Law firms are also seen as easy targets. [10] Law firms are perceived as being more vulnerable to cyber incursions than their clients, and indeed generally have "significantly less cybersecurity protection in place than their clients ...." [11] The FBI has called some law firms "clueless" when it comes to securing corporate data. [12] Others have labeled law firms "weak links" and "the soft underbelly of corporate cybersecurity." [13] Due to these perceived deficiencies, some clients themselves have taken on the responsibility of ensuring that their legal counsel's cybersecurity protocols are up to standard. [14]

While law firms will always be attractive targets to hackers seeking to steal valuable corporate information, law firms need not, and indeed must not continue ***1239** to let themselves be easily exploited. Lawyers and law firms play a critical role in the protection of their clients' data and have ethical duties both to secure data and to respond appropriately to data breaches. It is therefore of utmost importance that lawyers and law firms be informed about their ethical responsibilities in relation to technology.

This Note will examine some of the unique ethical standards that apply to lawyers in relation to technology and cybersecurity. The first section will discuss the lawyer's ethical obligation to secure client data, including the cybersecurity implications of the ethical duties of competency, confidentiality, safeguarding client data, communication, and supervision of lawyers and non-lawyers. The second section will argue that, despite the lack of an explicit rule requiring lawyers to report data security breaches to their clients, such a duty does in fact exist. This section will demonstrate how such an obligation may be derived from the existing ethical duties of a lawyer as a fiduciary. It will then examine an emerging trend among certain jurisdictions of explicitly embracing a duty to report data breaches. Finally, the second section will conclude by arguing for an amendment to current ethics rules that would explicitly adopt a duty to notify clients of data breaches.

I. LAWYERS' ETHICAL DUTIES TO SECURE CLIENT DATA

As with all aspects of a lawyer's representation of his or her clients, a lawyer's handling of client data is governed by a number of ethical rules. Those most relevant to the discussion of cybersecurity include the duties of confidentiality, competence, communication, and the supervision of lawyers and non-lawyers.

A. COMPETENCE

The first and most basic of ethical requirements applicable to a lawyer's use of technology is that of competence. The American Bar Association's *Model Rules of Professional Conduct*, Model Rule 1.1, states that "[a] lawyer shall provide competent representation to a client," and notes that "[c]ompetent representation requires the legal knowledge, skill thoroughness and preparation reasonably necessary for the representation." [15] In 2012, the ABA established the Ethics 20/20 Commission to perform a review of *Model Rules* in the context of advances in technology and global legal practice developments. [16] The Commission amended Model Rule 1.1 to emphasize that the duty of competence extends to a ***1240** lawyer's handling of technology. [17] Comment 8 to this rule now provides: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." [18] This rule and the corresponding comment make clear that understanding and responsibly handling technology is now a requirement for the ethical practice of law. [19] From email to wi-fi to portable electronic devices, attorneys must be aware of the inherent vulnerabilities of the technology they employ and must take appropriate steps to ensure that those vulnerabilities are not exploited. [20] The threat of a legal malpractice claim or bar discipline for incompetence with respect to technology has now become a real possibility, with some practitioners predicting that the duty of competence in technology could "become a new standard of practice in the context of legal malpractice." [21]

Learning the ins and outs of rapidly advancing technology may seem like a daunting task, especially for those attorneys who built their practices before the digital age. Fortunately for those less technologically inclined, the aim of the rules is not that every attorney in a practice be up to date on the latest technology and its vulnerabilities, but rather that clients are competently represented and reasonably protected from cyber exploitation. [22] Therefore, if an attorney is himself not competent to use a particular from of technology in a manner that reasonably protects client confidentiality, the duty of competency mandates that the lawyer seek appropriate outside help. [23]

*1241 Further, competence requires awareness of the ever-changing nature of technology. Actions taken to secure client data that may be reasonable now may not be enough to fulfill the duty of competence in the near future. As the New York State Bar Professional Ethics Committee notes, lawyers must "[p]eriodically review[] security measures as technology advances over time to ensure that the confidentiality of client information remains reasonably protected." [24] Thus, lawyers may not use ignorance as an excuse as to why they were unable to protect client confidences.

B. CONFIDENTIALITY

The enormous amount of confidential information stored in digital form today has caused inadvertent disclosure, whether by accident or as a result of cyberattack, to become a concern of great importance. [25] Lawyers have an ethical duty to use reasonable care to protect their clients' sensitive information. ABA Model Rule 1.6(a) states that "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent ...." [26] This obligation of client confidentiality is at the core of the attorney-client relationship, as it forms a basis of trust between the two parties. The duty applies equally to all varieties of confidential client information, including electronic correspondence and records. [27] Though a lawyer may never actively choose to reveal client data, this rule has been defined to create a duty to secure client data against reasonably foreseeable losses. [28] The Ethics 20/20 Commission amended Model Rule 1.6 to include a new subpart (c), which stipulates that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." [29] Comment 18 provides that any compromise of client data does not constitute a violation of subpart (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. [30] The Comment further explains that factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to:

*1242 • The sensitivity of the information;

• The likelihood of disclosure if additional safeguards are not employed;

• The cost of employing additional safeguards;

• The difficulty of implementing additional safeguards; and,

• The extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or program excessively difficult to use). [31]

With these new amendments, the Ethics 20/20 Commission recognized that lawyers "cannot guarantee security," and noted that the amendments do not impose on lawyers a duty "to achieve the unattainable." [32] Rather, the changes are intended to identify factors that can aid lawyers in determining whether their data security measures are reasonable. [33]

The duty of confidentiality does not end when representation ceases, but rather extends to former clients as well. Model Rule 1.9 states, "[a] lawyer who has formerly represented a client in a matter ... shall not thereafter ... reveal information relating to the representation ...." [34] This Rule by implication obligates lawyers to exercise reasonable care when discarding devices with stored electronic information. [35] The duty of competence requires that lawyers "keep abreast of ... the benefits and risks associated with relevant technology." [36] One of the risks inherent in the disposal of technology is that data still existing on old hard disks may be lifted and misappropriated. The ABA Lawyer's Manual on Professional Conduct stipulates that a lawyer who uses technology with electronic storage media "must obtain adequate assurances or take reasonable steps to ensure that clients' confidential information is removed from the devices before they are ... disposed of. The lawyer must supervise employees and outside technicians who have access to the devices to ensure that they protect confidential information." [37] Lawyers must therefore ensure that their method of disposal of old technology protects the privacy of both former and ***1243** current clients. [38]

C. COMMUNICATION

Model Rule 1.4, Communications, is also relevant to lawyers' use of technology. [39] The Rule requires attorneys to "reasonably communicate with clients about the means by which the client's objectives are to be accomplished." [40] This rule implies that attorneys should reasonably inform clients about the law firm's modes of client communication, including communication technology. [41] In Formal Opinion 2011-200, the Pennsylvania Bar comments that "[w]hile it is not necessary to communicate every minute detail of a client's representation, 'adequate information' should be provided to the client so that the client understands the nature of the representation and 'material risks' inherent in an attorney's methods." [42] For example, the opinion continues, "it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of 'cloud computing' and the advantages as well as the risks endemic to online storage and transmission." [43]

Moreover, informing clients of the forms of communication employed by the law firm may also help lawyers comply with their duty of confidentiality. Advising clients about communication technology may allow them to assess for themselves whether their security needs are being met or whether additional ***1244** safeguards are necessary to keep data confidential. [44]

Additionally, Model Rule 1.4 requires lawyers to "keep the client reasonably informed about the status of the matter." [45] This provision arguably requires notifying clients in the case of a data breach involving client information. [46]

D. SUPERVISION OF LAWYERS AND NON-LAWYERS

Supervising attorneys have an ethical duty to ensure that those who work under them conform to all standards of the *Model Rules*. Model Rule 5.1 provides that lawyers with managerial authority "shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct." [47] Model Rule 5.3 is substantially similar, but applies to the supervision of non-lawyers, requiring supervising attorneys to "make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer." [48] These rules taken together reflect the idea that everyone that plays a role in client services needs to be involved in managing cybersecurity risk. [49] After all, cybersecurity measures are only as strong as a firm's weakest link. Model Rule 5.3 also mandates that attorneys in managerial roles ensure that those working under them understand how their ethical duties extend to the technology with which they work. The New York State Bar suggests this means that supervising attorneys should, among other things, distribute and regularly update a written data security policy, limit access to certain sensitive

client information to specific employees by using encrypted passwords, require personnel to regularly change their passwords, and coordinate all information security policies with internal or trusted outside IT staff. [50]

Model Rule 5.3 has also been interpreted to apply to any service that a lawyer uses in the course of his representation of a client. [51] The commentary to Model Rule 5.3 now specifically refers to "internet based service [s]," and states that a lawyer "must make reasonable efforts to ensure that the services are provided in a ***1245** manner that is compatible with the lawyer's professional obligations." [52]

E. SAFEGUARDING CLIENT PROPERTY

Implicit in the obligations of competence, confidentiality, and supervision of lawyers and non-lawyers is the duty to safeguard client property. This duty is made explicit by Model Rule 1.15, which states, "[a] lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property .... Other property shall be identified as such and appropriately safeguarded." [53]

This rule has potential implications for the Bring Your Own Device (BYOD) trend, by which law firms have increasingly allowed lawyers to work on client issues using their own computers, tablets, and mobile phones. [54] Depending on how BYOD policies are implemented, lawyers who store client data on their personal electronic devices may violate Model Rule 1.15 by failing to separate their own property from that of their clients. This rule is especially pertinent considering that more than one third of data breaches occur as a result of theft of loss of electronic storage devices. [55] The loss or theft of a personal device on which a lawyer has sensitive client data could have serious legal and ethical implications. [56]

F. STANDARDS FOR "REASONABLE EFFORTS"

The *Model Rules*, as well as state bar rules and ethics opinions, emphasize the importance of making "reasonable efforts" to secure client data, but what exactly does "reasonable" mean? Ethics authorities have largely shied away from outlining specific steps that attorneys can take to ensure the reasonableness of their security measures due to the fact that what is reasonable changes over time. [57] Nevertheless, the ABA and several state bar associations have provided some guidance on what might constitute reasonable care in certain scenarios. [58] *The ABA Cybersecurity Handbook* outlines several "top considerations" for lawyers and law firms to ensure compliance with their ethical duties surrounding ***1246** the protection of client data. [59] Among these are: (1) conducting a risk assessment; (2) appropriately encrypting sensitive data; (3) appropriately securing mobile devices; (4) restricting network access to known users and devices; (5) developing a data destruction plan; and (6) preparing for a data breach incident. [60] Each of these steps should be a basic part of a law firm's reasonable and comprehensive cybersecurity strategy.

1. PERFORMING A RISK ASSESSMENT

One of the most basic steps that lawyers can take to ensure compliance with their ethical duties regarding cybersecurity is to perform a risk assessment considering the factors included in Comment 18 to Model Rule 1.6. [61] Implementing policy based on a calculated risk assessment allows firms to manage their most serious vulnerabilities and avoid worst-case scenarios. [62] Without a comprehensive risk-based strategy, firms are likely to waste scarce resources in defending against less serious threats while leaving more serious avenues for harm inadequately defended. [63] In assessing risk, a lawyer must calculate the likelihood that a threat will materialize, the potential harm it could cause, the cost of preventing that harm, and the sufficiency of the firm's policies, procedures, and defenses against the threat. [64] For example, a common means

by which client data is compromised is by the loss or theft of mobile devices containing such data. [65] Understanding the likelihood and potential gravity of such a threat, a law firm which seeks to act reasonably to protect client data may opt to require data encryption on mobile devices. [66] Conversely, for small firms handling personal matters, the likelihood that information may be compromised through an email hack may be low; therefore, it may be reasonable for the firm to forgo encrypting all of its email correspondence. [67] As cyber threats are continually evolving, risk ***1247** assessment should be an ongoing process in which firms periodically reevaluate potential threats and the efficacy of security measures. [68]

2. ENCRYPTING SENSITIVE DATA

Encryption is the most commonly used means of securing confidential information. [69] As theft or inadvertent loss of mobile devices is one of the greatest threats to the security of client data, [70] the use of appropriate encryption technology on such devices generally constitutes a reasonable precaution. [71] Moreover, encryption is a relatively inexpensive tool [72] whose benefits generally greatly outweigh its cost of implementation. [73] The New York State Bar Association generally recommends "[a] near impenetrable encryption system on firm networks and individual computers for accessing confidential and sensitive client information," as well as "[a] mechanism so that such confidential information remains encrypted in the event electronic documents are 'checked out' from the firm's ... servers." [74] Similarly, the State Bar of Arizona recommends lawyers to "consider firewalls, password protection schemes, encryption, anti-virus measures," and other related measures. [75] Moreover, ethical standards aside, encrypting client data may explicitly exempt law firms from many state statutes requiring notification of affected parties in the event of a breach of personal data. [76] It is therefore reasonable and prudent for lawyers to implement basic encryption programs on devices that store sensitive client information.

3. APPROPRIATELY SECURING MOBILE DEVICES

In addition to encryption, firms that permit lawyers to work on their own mobile devices should have in place some form of Mobile Device Management to remotely lock, erase, and check the geographic location of such devices if they become lost or stolen. [77] If implementing this technology is infeasible, [78] a firm ***1248** may either issue work devices--which make security management easier [79] --or institute a policy restricting the use of mobile devices to store client data.

4. RESTRICTING NETWORK ACCESS

Lawyers have the duty to "make reasonable efforts to prevent ... unauthorized access to [client] information." [80] Restricting network access to only known users and devices is one common sense method of fulfilling this duty that costs little and pays dividends in terms of security. A first step to ensuring only authorized users have access to client data is adopting a password policy that ensures adequate passwords and periodic updates. [81] *The ABA Cybersecurity Handbook* suggests using a different password for each device, as well as for each website that a lawyer visits. Additionally, law firms should prohibit the use of "jailbroken" or "unteathered" devices, which may allow unauthorized third parties access to a firm's network. [82]

5. DEVELOPING A DATA DESTRUCTION PLAN

The lawyer's duty to keep client data confidential does not end when the lawyer disposes of that data, or of the device on which that data is stored. [83] It is therefore reasonable that firms develop policies to ensure that any discarded or

reused electronic storage devices be free of harvestable client data. [84] Furthermore, several laws and regulations impose requirements mandating that data be disposed of in secure ways. [85] These statutes usually require law firms to implement and enforce policies requiring the permanent destruction of electronic records containing personal information. [86]

6. PREPARING FOR A DATA BREACH INCIDENT

Even when reasonable precautions are taken, there will still be instances in which a determined cybercriminal will be able to access confidential client files. In such worst-case scenarios, lawyers still have the duty to act reasonably to mitigate the damage. [87] Once a breach is discovered, acting quickly to locate its source and notify appropriate parties may help to stem the loss of confidential ***1249** data. [88] The ABA recommends creating a plan to address a potential data breach by understanding which data breach notification laws might be applicable and what they require, [89] and by liaising with Internet service providers, law enforcement, and other security providers to ensure a swift response. [90]

II. IN THE EVENT OF A BREACH

While ethics rules have been updated to address securing electronic client information, they have been largely silent on what, if any, ethical duties exist in the event of a data breach. This section will argue that, despite this silence, lawyers have an ethical duty derived from their role as fiduciaries to report data security breaches to affected clients. The section will then examine an emerging trend among state bar associations of imposing such duties on lawyers in the event of a loss of client data by third party vendors. It will assert that this trend represents a positive development towards a duty to notify, but should be expanded both in scope and implementation. Lastly, this section will argue that the *Model Rules* should be amended to include an explicit duty to report the material loss or compromise of client electronic information.

A. DUTY TO DISCLOSE A DATA BREACH

Though no rule may specifically mandate that an attorney disclose a data breach to a client, the spirit of the *Model Rules* does impose such a duty. The *Model Rules* were expounded on the premise that lawyers have a fiduciary relationship with their clients. [91] A fiduciary is "one who voluntarily holds a position of special trust and confidence that obliges the fiduciary to act in the best interest of another." [92] Included in the fiduciary duty are the principles of loyalty and candor. [93]

1. DUTY OF LOYALTY

Comment 5 to Model Rule 1.8 explains that the "[u]se of information relating to the representation to the disadvantage of the client violates the lawyer's duty of loyalty." [94] There can be little doubt that withholding information regarding a ***1250** material loss or compromise of client data constitutes a use of that information to the disadvantage of the client. A data breach can have considerable consequences, with potential injuries ranging from identity theft to misappropriation of trade secrets, reputational harm, or loss of market share. While disadvantageous in any event, these outcomes may deteriorate if not swiftly acted upon. [95] The Federal Trade Commission has found that the longer identity theft goes undetected, the greater the harm that usually follows. [96] If a lawyer's duty of loyalty requires him to act in the best interest of his client, it follows that the lawyer has a duty to reveal a data security breach so that the client may mitigate any harm.

Withholding information about a data breach may also present a conflict of interest. Comment 1 to Model Rule 1.7 explains that "[c]onflicts of interest can arise from ... the lawyer's own interests." [97] It is in the best interest of the client to

know if his confidential information has become compromised; however, it is in the lawyer's interest to avoid potential litigation and reputational sanction stemming from the breach. This conflict has been called the "disclosure disincentive," as disclosure of a breach makes traceable an otherwise undiscovered breach and is fundamentally at odds with the lawyer's desire to avoid sanction. [98] In cases of conflict, the *Model Rules* dictate that the lawyer, as a fiduciary, must put the client's interest before his own. [99]

2. DUTY OF CANDOR

The duty of candor, captured in Model Rule 1.4, requires that a lawyer "keep the client reasonably informed about the status of the matter" [100] and "explain [the] matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." [101] Surely the "status of the matter" could be materially affected by a loss or compromise of client files. This is perhaps especially true of corporate deals, such as mergers and acquisitions, where a data breach may materially affect stock prices and/or the likelihood of a deal's success. Further, this kind of information is crucial so that the client may ***1251** make informed decisions regarding his or her representation. A data breach may require a change in strategy or may prompt a client to search for alternative representation offering a higher level of data security. According to Lucian Pera, a partner at Adams & Reese LLP, even in the absence of an explicit ethics rule, "attorneys still have a fiduciary duty to clients that requires them to be candid about these issues." [102] "If ... [a] client's private confidential information has been released into the world, that seems like a pretty material development in their representation." [103]

Ultimately, withholding information about a material data breach puts the lawyer in a position inimical to his duties as a fiduciary. It violates the duty of loyalty by acting against the client's best interest in situation of a conflict of interest; it violates the duty of candor by withholding information of likely significance to the client; and, it violates the trust that the client has placed in the lawyer as a fiduciary.

B. AN EMERGING TREND

Though the *Model Rules* remain devoid of explicit ethical duties governing attorney behavior in the event of a breach, [104] the ABA and a small number of state bar associations have begun to explicitly adopt the duties that already exist implicitly within the *Model Rules*. In Formal Opinion 95-398, the ABA found that "should a significant breach of confidentiality occur within a computer maintenance company, accounting firm, or the like, a lawyer may be obligated to disclose such breach to the client or clients whose information has been revealed." [105] Tying this obligation to the lawyer's duty of candor, the opinion added, "[w]here the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Model Rule 1.4(b)." [106] Recently some state bar associations have begun to explicitly incorporate this duty as well. In Ethics Opinion 842 (2010), the New York State Bar Association ruled that a lawyer who learns of a "breach of confidentiality by [an] online storage provider ... must investigate whether there has been any ***1252** breach of his or her own clients' confidential information, [and] notify any affected clients ...." [107] Alaska Rule 5.3(d) (2014) dictates that "[a] lawyer who learns that any person employed by the lawyer has revealed a confidence ... protected by these rules shall notify the person whose confidence or secret was revealed." [108] Pennsylvania Ethics Opinion 2011-46 (2011) provides that a lawyer who neglects to remove client data upon disposing of a hard drive "may have a duty to notify clients." [109]

Though these opinions appear to be pioneers of an emerging duty to disclose data breaches to those affected, they remain limited in scope and have yet to be widely adopted. ABA Formal Opinion 95-398, New York Ethics Opinion 842 and

Alaska Rule 5.3(d) are all restricted to scenarios where a third party suffers a breach and provide no clues as to what duties may apply in the event that a law firm itself suffers a breach.

C. AN EXPLICIT DUTY NEEDED

In order to mitigate the disclosure disincentive and adequately protect client interests, the ABA should follow the lead of New York and Alaska Bar Associations and amend the *Model Rules* to explicitly include an ethical duty to report material data breaches to clients. Such a duty could be modeled after current legal duties and would have the dual effect of incentivizing lawyers to implement adequate security measures and helping clients mitigate the harm caused by a security leak.

Currently, the only clear duties that exist prescribing behavior in the event of a breach are statutory. Nearly all states have passed security breach notification laws, most of which are based on a 2002 California law requiring entities to notify individuals of any unauthorized acquisition of their personal information. [110] Additionally, Health Insurance Portability and Accountability Act (HIPAA) regulations require notification for a breach of health data, and requirements of federal banking regulatory agencies mandate notification for compromised financial data. [111] These laws "impose an obligation similar to the ***1253** common law duty to warn of dangers, which is often based on the view that a party who has superior knowledge of a danger of injury or damage to another posed by a specific hazard must warn those who lack such knowledge." [112] Though they provide a good model for a broader duty, these laws do not go far enough to protect lawyers' clients. These laws only apply to the limited scenario in which individuals' personal information--including name, SSN, credit card data, etc.--has been compromised. [113] They do not require disclosure of breaches that affect non-personal corporate data, such as merger plans or trade secrets.

A broader, explicit ethical duty is needed. Like existing legal obligations, an ethical duty would require notice to clients who might be adversely affected by a breach. Such a duty would be based on the lawyer's role as a fiduciary and would extend to breaches of all types of client data, not just personal information. The ABA has called it "an open secret that law firms have played breaches very close to the vest"--a problematic fact for clients trying to secure data. [114] An explicit fiduciary duty would subordinate lawyers' fear of liability or reputational sanction to the interests of the client, providing the client with the opportunity to take remedial action to mitigate the consequences of a breach. Moreover, it would provide an additional incentive for lawyers to ensure the adequacy of their security measures. Scholars have established that both individuals and businesses can be significantly affected by the broadcasting of information about their past behavior. [115] If lawyers are aware that they must disclose security breaches to their clients who then in turn may look elsewhere for legal services, they are likely to take the necessary steps to ensure that a breach will not occur. [116]

D. FORM OF THE DUTY

If a duty is adopted, there is some debate about what it should look like. Some states, such as California, have enacted breach notification statutes that require notification upon a reasonable belief of unauthorized access to the consumer's personal information. [117] Others, such as North Carolina, require notification only if there is a reasonable likelihood of misuse of the leaked information. [118] An ethical duty to report a breach to a client should follow the latter model.

Though a duty of complete candor would simplify the process of determining whether or not to report a breach, it poses a risk of needlessly alarming or ***1254** over-warning clients. Data breaches can be extremely complicated and bewildering affairs. It is often difficult to determine when and where a breach originated, as well as whether data was actually compromised. In the event of a breach, the difficulty of ascertaining whether the incident warrants notifying clients or poses no risk to confidential client information seems to weigh in favor of a *per se* rule of complete candor.

Such a rule would circumvent the difficult process of determining the nature of the breach and would ensure that, in the case of an underestimation of the gravity of a security lapse, clients remain in the best position to mitigate the effects of the breach.

However, in an environment of increasingly common cybercrime, such a *per se* rule would risk an inundation of notifications from law firms, both wasting law firm resources and reducing the effectiveness of warnings. A federal guideline for breach notification by financial institutions states that "notification might needlessly alarm customers where little likelihood of harm exists," and "frequent notices in non-threatening situations would be perceived by customers as routine and commonplace, and therefore reduce their effectiveness." [119] Moreover, such notices would require an enormous commitment of time and resources from law firms collectively and may unnecessarily strain relationships with clients. Under a *per se* rule, anytime a breach were suspected, a law firm would be required to send a notice to the client that his or her information may have been compromised. This task would sidetrack the lawyer and perhaps needlessly cause the client to think that the law firm has not adequately protected his or her data.

Though more tedious, an ethical rule requiring notification only in the case of a reasonable likelihood of misuse of compromised data is superior to a *per se* rule. Such a rule would grant law firms a high level of discretion to decide whether or not misuse would occur. This would obviate the need for mass notifications for low-level breaches, avoiding the problem of ineffective notice caused by over-notification. Such a balancing test would also still provide clients with adequate protection against serious breaches, because lawyers, as fiduciaries, would be required to notify clients of any breach that could reasonably materially affect their interests.

CONCLUSION

The pace of technological advancement is dizzying. That which is state-of-the-art today may be obsolete by tomorrow. As both technological capabilities and threats evolve, so too must the practice of law. Lawyers' basic ethical duties remain the same. As fiduciaries, lawyers must act in their clients' best interests. ***1255** They must at all times be loyal and candid, competently represent their clients, and effectively safeguard their clients' confidences. However, the application of these duties to an increasingly cyber practice represents a new and complex challenge. Lawyers seeking to fulfill their ethical duties must strive to maintain technological competence in their practices, either by learning the advantages and vulnerabilities of new technology themselves, or by employing someone familiar with them. They must communicate the benefits and risks of these technologies to their clients, so that clients may make informed decisions regarding their representation. Lawyers must take reasonable steps to safeguard their clients' privileged information, taking into account the sensitivity of that information and the costs and benefits of employing additional security measures. Lawyers must be accountable for those in their employ, always ensuring that both employees and contractors take necessary steps to protect client confidences. Lastly, lawyers must inform clients in the event that confidential information is materially compromised. Such a duty is implicit in the *Model Rules* and should be made unequivocal so as to avoid misunderstanding. By following these rules and always acting with reasonableness, lawyers should be better equipped to handle the ethical challenges of an increasingly cyber practice.

Footnotes

a1 J.D., Georgetown University Law Center (expected May 2017); B.A., University of North Carolina at Chapel Hill (2009).

1 *See* Bree Fowler, *Study Cites Cybercrime's Rising Costs to Corporations*, ASSOCIATED PRESS (Oct. 6, 2015), http://bigstory.ap.org/article/b312c7a90b934c05918363e18fd9aecb/study-cites-cybercrimes-rising-costs-corporations [https://perma.cc/7SYG-9NHD]; *see also Net Losses: Estimating the Global Cost of Cybercrime*, CTR. FOR STRATEGIC & INT'L

STUD. (June 2014), http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf [https://perma.cc/A5CL-VS84] (noting that cybercrime costs the global economy more than $400 billion each year).

2 *See, e.g.*, Susan Hansen, *Cyber Attacks Upend Attorney-Client Privilege,* BLOOMBERG BUSINESSWEEK (Mar. 19, 2015), http://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security [http://perma.cc/6JJT-BR99].

3 *See* Michael A. Riley & Sophia Pearson, *China-based Hackers target Law Firms to Get Secret Deal Data*, BLOOMBERG (Nov. 5, 2015), http://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-target-law-firms [http://perma.cc/YGC8-YDBJ]; *see also* Hansen, *supra* note 2; Debra Cassens Weiss, *Some NY Law Firm Reps Said to Be Clueless as FBI Warned of Hackers Seeking Corporate Data*, A.B.A. J. (Jan. 31, 2012), http://www.abajournal.com/news/article/some_ny_law_firm_reps_said_to_be_clueless_as_fbi_warned_of_hackers_seeking_/ [https://perma.cc/9PC9-JXHD] ("In Canada, seven law firms were hit in 2010 by Chinese-based hackers who were apparently trying to derail a $40 billion corporate acquisition ....").

4 *See* Matthew Goldstein, *Citigroup Report Chides Law Firms for Silence on Hackings*, N.Y. TIMES (Mar. 26, 2015) (Puckett & Faraj, a DC-based firm, "was hacked in 2012 by activists associated with the group Anonymous, who were angered by the firm's representation of a United States soldier who pleaded guilty in connection with his role in the death of 24 Iraqi civilians ....").

5 *See* Sharon D. Nelson, David G. Ries & John W. Simek, *Law Firm Data Breach Nightmares and How to Prevent Them*, A.B.A., BRIEF, Spring 2013, at 17.

6 *See* Matthew Goldstein, *supra* note 4; *see also* Nelson, Ries & Simek, *supra* note 5, at 17 (noting that the ABA's *2012 Legal Technology Survey Report* found that 15.4 percent of law firms with ten to forty-nine lawyers had experienced some kind of security breach in the past.).

7 *See* Alan W. Ezekiel, *Hackers, Spies, and Stolen Secrets: Protecting Law Firms From Data Theft*, 26 HARV. J.L. & TECH. 649, 650 (2013).

8 *Id.*

9 JANE LECLAIR & GREGORY KEELEY, CYBERSECURITY IN OUR DIGITAL LIVES 128 (2015).

10 *See* Drew Shimshaw, *Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data*, 38 AM. J. TRIAL ADVOC. 549, 550 (2015); *see also* Weiss, *supra* note 3 (Mary Galligan, head of FBI cyber division said, "As financial institutions in New York City and the world become stronger, a hacker can hit a law firm and it's a much, much easier quarry ...."); John Reed, *The New Cyber Vulnerability: Your Law Firm*, FOREIGN POL'Y (Nov. 7, 2012), http://foreignpolicy.com/2012/11/07/the-new-cyber-vulnerability-your-law-firm/ [https://perma.cc/A93R-HLWW] (law firms described as "pretty much the perfect place to steal data from.").

11 JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 105 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].

12 *See*Weiss, *supra* note 3.

13 Shimshaw, *supra* note 10, at 551.

14 *See* Goldstein, *supra* note 4.

15 MODEL RULES OF PROF'L CONDUCT R. 1.1 (2010) [hereinafter MODEL RULES].

16 *See ABA Commission on Ethics 20/20 Introduction and Overview*, A.B.A., http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introdution_and_overview_report.authcheckdam.pdf [https://perma.cc/N385-HJHK] (last visited Aug. 11, 2016).

17 *See id.* The Ethics 20/20 report noted the significance of the competent use of technology by lawyers in the digital age: "First, technology has irrevocably changed and continues to alter the practice of law in fundamental ways .... Lawyers must understand technology in order to provide clients with the competent and cost-effective services that they expect and deserve .... Because of the sometimes bewildering pace of technological change, the Commission believes that it is important to make explicit that a lawyer's duty of competence, which requires the lawyer to stay abreast of changes in the law and its practice, includes understanding relevant technology's benefits and risks." AM. BAR ASS'N, COMMISSION ON ETHICS 20/20, at 3, 8 (2012).

18 MODEL RULES R. 1.1 cmt. 8.

19 *See* MODEL RULES R. 1.1 cmt. 8.

20 *See, e.g.*, MODEL RULES R. 1.1.

21 Catherine J. Lanctot, *Becoming a Competent 21st Century Legal Ethics Professor: Everything you Always Wanted to Know about Technology (But Were Afraid to Ask)* 11 (Villanova Univ. Sch. of Law, Pub. Law & Legal Theory, Working Paper No. 2015-1001, 2014). Lanctot moreover notes that at a LegalTech conference in New York in 2014, a panel of federal judges warned practitioners that those who neglect to become technologically proficient could be committing "slow career suicide." *Id.*

22 *See, e.g.*, MODEL RULES R. 1.1 cmt. 2.

23 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 66. Many state bar associations have also incorporated the requirement to obtain help into their rules of professional conduct or ethics opinions. *See, e.g.*, State Bar of Ariz., Op. No. 05-04 (July 2005), http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=523 [https://perma.cc/58U7-TJR5] ("[I]f an attorney lacks or cannot reasonably obtain [the] competence [to ensure that client confidences are not disclosed to third parties, he must] retain an expert consultant who does have such competence."); State Bar of Cal., Formal Op. No. 2010-179 (2010), http://www.calbar.ca.gov/LinkClick.aspx?fileticket=odIjrEe0wjI%3D&tabid=2167 [https://perma.cc/5GC5-GWVL] (last visited Aug. 11, 2016) ("If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.").

24 N.Y. State Bar Prof'l Ethics Comm., Op. No. 842 (2010), https://www.nysba.org/CustomTemplates/Content.aspx?id=1499 [https://perma.cc/N8Z2-FXD3] (last visited Aug. 11, 2016); *see also* State Bar of Ariz. Ethics Op. 09-04 (Dec. 2009), http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=704 [https://perma.cc/SGQ2-7Q4K] ("Competent personnel should conduct periodic reviews to ensure that security precautions in place remain reasonable as technology progresses.").

25 *See* Lanctot, *supra* note 21, at 19.

26 MODEL RULES R. 1.6(a).

27 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 62.

28 *See* MODEL RULES R. 1.6 cmts. 18, 19.

29 MODEL RULES R. 1.6(c).

30 *See* MODEL RULES R. 1.6 cmt. 18.

31 *See* MODEL RULES R. 1.6 cmt. 18.

32 Allison Grande, *ABA Group Floats Tougher Data Security Rule For Attys*, LAW360 (May 14, 2012), http://www.law360.com/articles/340080/aba-group-floats-tougher-data-security-rule-for-attys [https://perma.cc/6MYP-VGS5].

33 *See* Louise Lark Hill, *Cloud Nine or Cloud Nein? Cloud Computing and Its Impact on Lawyers' Ethical Obligations and Privileged Communications*, PROF. LAW. 109, 119 (2013).

34 MODEL RULES R. 1.9.

35 *See, e.g.*, Stephen Wu, *Attorneys Have an Obligation to Clean Up Their Act--And Their Media*, RSA CONF. (Jan. 2011), http://www.rsaconference.com/blogs/attorneys-have-an-obligation-to-clean-up-their-act-and-their-media#sthash.vacn5El3.dpuf [http://perma.cc/DHR2-N2QJ].

36 MODEL RULES R. 1.1 cmt. 8.

37 29 Law. Man. Prof. Conduct (ABA/BNA) 520 (2013), http://www.americanbar.org/content/dam/aba/events/communications_law/2014/02/forum-on-communications-law-19th-annual/hotissuesinethics/protecting_client_info_in_electronic_age.authcheckdam.pdf [https://perma.cc/4CN8-LE9J].

38 *See, e.g.*, Ala. Ethics Op. 2010-02, https://www.alabar.org/resources/office-of-general-counsel/formal-opinions/2010-02/ [https://perma.cc/5QVR-P3WM] (holding that lawyers should ensure that confidential data has been removed when discarding electronic media); Fla. Ethics Op. 10-2 (2010), http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+10-2!OpenDocument&Click= [https://perma.cc/QNW4-HQXR] (last visited Aug. 11, 2016) (holding that lawyers using devices with electronic storage must ensure removal of clients' confidential data before devices are sold, returned to lessor, or otherwise discarded); Ill. Ethics Op. 12-06 (2012), https://www.isba.org/sites/default/files/ethicsopinions/12-06%20pdf.pdf [https://perma.cc/DAH3-CC8D] (last visited Aug. 11, 2016) (holding that when disposing of files, lawyers must ensure client data remains confidential).

39 *See, e.g.*, Shimshaw, *supra* note 10.

40 MODEL RULES R. 1.4(a).

41 *See* David G. Ries, *Cyber Security for Attorneys: Understanding the Ethical Obligations*, L. PRAC. TODAY (Mar. 2012), http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/march12/cyber-security-for-attorneys-understanding-the-ethical-obligations.html [https://perma.cc/AQ55-ADKA].

42 Pa. Bar Assoc., Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200, http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf [https://perma.cc/HA2C-LX42] (last visited Aug. 11, 2016).

43 *Id.*; *see also* N.H. Bar, Ethics Comm., Advisory Op. No. 2012-13/4 (Feb. 21, 2013), https://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp [https://perma.cc/4K6W-HX4E] ("Where highly sensitive data is involved, it may become necessary to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent.").

44 *See* MODEL RULES R. 1.6 cmt. 18 ("A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.").

45 MODEL RULES R. 1.4(a).

46 *See* Ries, *supra* note 41; *infra* Part II.A.

47 MODEL RULES R. 5.1.

48 MODEL RULES R. 5.3.

49 *See* Michael McNerney & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, 62AM. U. L. REV. 1243, 1266 (2013).

50 *See Attorney Professionalism Forum,* 86 N.Y. ST. B.J. 50, June 2014, at 52.

51 *See* Shimshaw, *supra* note 10, at 563.

52 MODEL RULES R. 5.3. ("The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.").

53 MODEL RULES R. 1.15.

54 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 144, 164.

55 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 16.

56 The ABA acknowledges that employee use of personal devices for work-related purposes is "a practical reality," but encourages firms to adopt a data security plan that provides appropriate security controls for such devices. *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 147.

57 *See* Shimshaw, *supra* note 10, at 562.

58 *See* Hill, *supra* note 33, at 132.

59 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 33.

60 *Id.*

61 The sensitivity of the information, likelihood of disclosure if additional safeguards are not employed, cost of employing additional safeguards, difficulty of implementing safeguards, and extent to which safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). *See supra* Part I.B.

62 *See* McNerney & Papadopoulos, *supra* note 49, at 1266.

63 *Id.*

64 *See* Steven C. Bennett, *Data Security Breaches: Problems and Solutions*, 54 PRAC. LAW. no. 6, Dec. 2008, at 39, 41.

65 *See, e.g.*, ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 16.

66 The research company Garner noted that encryption can cost as little as $6 per account, whereas cleanup after a breach may be as costly as $90 per account. *See* Bennett, *supra* note 64, at 41.

67 However, email encryption may be a reasonable choice for highly sensitive data. *See* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf [https://perma.cc/E4V8-5KVH] (last visited Aug. 11, 2016) (noting that "[r]egular email is not a secure method for sending sensitive data").

68 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 31.

69 *See* Bennett, *supra* note 64, at 41.

70 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 16.

71 *See id.* at 34.

72 *See* State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2010-179 (2010), http://jolt.richmond.edu/wp-content/uploads/13-State-Bar-of-California-Opinion-2010-179-L0563533x7A34B.pdf [https://perma.cc/2F33-C8QV] (last visited Aug. 11, 2016).

73 *See* Meghan C. Lewallen, *Cloud Computing: A Lawyer's Ethical Duty to Act with Reasonable Care When Storing Client Confidences "In the Cloud"*, 60 CLEV. ST. L. REV. 1133, 1160 (2013).

74 *Attorney Professionalism Forum, supra* note 50, at 50, 52.

75 State Bar of Ariz., Ethics Op. 09-04 (Dec. 2009), http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=704 [https://perma.cc/77UF-32UT].

76 *See, e.g.*, Cal. Civ. Code § 1798.82(e); N.C. Gen. Stat. § 75-61(14).

77 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 19.

78 The price of this service may be beyond the reach of some smaller firms. *See* Sharon D. Nelson & John W. Simek, *How Lawyers Can Better Manage Their Technology*, 41 L. PRAC., no. 3, May/June 2015, at 26, 28.

79 *See id.*

80 MODEL RULES R. 1.6(c).

81 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 34.

82 *See id.*

83 *See supra* Part I.B.

84 *See supra* note 34 and accompanying text.

85 *See, e.g.*, Cal. Civ. Code § 1798.81; Mass. Gen. Laws ch. 93I.

86 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 58.

87 *See infra* Part II.

88 *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 141.

89 *See id.* at 142.

90 *See id.* at 34.

91 *See* MODEL RULES R. 1.15 cmt. 1; MODEL RULES R. 1.8 cmt. 17.

92 Brandon Faulkner, *Hacking into Breach Notification Laws*, 59 FLA. L. REV. 1097, 1122 (2007) (quoting Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 280 (2005)).

93 *See id.*; *see also* MODEL RULES R. 1.7 cmt. 1 ("Loyalty and independent judgment are essential elements in the lawyer's relationship to a client.").

94 MODEL RULES R. 1.8 cmt. 5.

95 *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 917 (2007).

96 *See id.* at 942.

97 MODEL RULES R. 1.7 cmt. 1.

98 *See* Schwartz & Janger, *supra* note 95, at 928.

99 *See generally* MODEL RULES R. 1.7, 1.8.

100 MODEL RULES R. 1.4(a)(3). Though 1.4(a) appears applicable only to explaining the "matter" at hand, comment 5 clarifies that "[t]he client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued .... The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation." MODEL RULES R. 1.4 cmt. 5.

101 MODEL RULES R. 1.4(b).

102 Allison Grande, *5 Steps To Take When Your Firm Is Hacked*, LAW360 (July 22, 2014), http://www.law360.com/articles/556398/5-steps-to-take-when-your-firm-is-hacked [https://perma.cc/RAE9-E94F].

103 *Id.*; *see also* Ries, *supra* note 41 (interpreting Rule 1.4 to require disclose of a data breach); Ill. State Bar Assoc., Advisory Op. 10-01 (July 2009), https://www.isba.org/sites/default/files/ethicsopinions/10-01.pdf [https://perma.cc/YK86-VN2Q] (finding that Rule 1.4 implies a duty to disclose a data breach).

104 MODEL RULES R. 1.6 cmt. 18 ("Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as ... laws that ... impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.").

105 ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995) (citing Model Rule 1.4(b)).

106 *Id.*

107 N.Y. State Bar Assoc., Ethics Op. 842, question 10 (Sept. 10, 2010), http://www.nysba.org/CustomTemplates/Content.aspx?id=1499 [https://perma.cc/K33D-DXHG].

108 ALASKA BAR RULES, Rule 5.3(d), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwin15acruHKAhUO42MKHdvyDyYQFggdMAA&url=https%3A%2F%2Fwww.alaskabar.org%2Fservlet%2Fdownload%3Fid%3D2499&usg=AFQjCNGJhBkogN8hCnr0Qg_EIZTPfRE1wQ&sig2=x06feTRKxNpKUL7SY5TtiA [https://perma.cc/Z7PN-GXV5].

109 E-mail from Susan Michmerhuizen, Research Lawyer, ABA ETHICSearch, to author (Nov. 5, 2015) (on file with author).

110 *See* Faulkner, *supra* note 92, at 1104.

111 *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Part III of Supplement A to Appendix, at 12 C.F.R. Part 30 (OCC), Supplement A to Appendix D-2, at 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), 70 Fed. Reg. 15736-15754 (March 29, 2005).

112 *Id.*

113 *See id.*

114 Nelson, Ries & Simek, *supra* note 5, at 19.

115 *See* Schwartz & Janger, *supra* note 95, at 929.

116 *See* Bennett, *supra* note 64, at 44 ("Fifty-eight percent of surveyed customers stated that they lost confidence in the [breached] company after notification, and 31 percent terminated their relationship with the organization that lost the data.").

117 *See* Schwartz & Janger, *supra* note 95, at 935.

118 *See* Faulkner, *supra* note 92, at 1108.

119 *See* Schwartz & Janger, *supra* note 95, at 939 (quoting Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,740 (Mar. 29, 2005)); *id.* at 916 (noting that the Washington Post has editorialized against these kinds of notifications as creating "'tedious warnings' that will cause people to 'ignore the whole lot'").

End of Document

Exhibit "4"

West's Annotated California Codes
Civil Code (Refs & Annos)
Division 3. Obligations (Refs & Annos)
Part 4. Obligations Arising from Particular Transactions (Refs & Annos)
Title 1.81. Customer Records (Refs & Annos)

West's Ann.Cal.Civ.Code § 1798.82

§ 1798.82. Person or business who owns or licenses computerized data including personal information; breach of security of the system; disclosure requirements

Effective: January 1, 2017
Currentness

(a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]

Date:
[insert date]

NOTICE OF DATA BREACH

What Happened?

What Information Was Involved?

What We Are Doing.

What
You Can
Do.

Other Important Information.
[insert other important information]

Call [telephone number] or go to [Internet Web site]

For More
Information.

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). [1] However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(i)(1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the person or business has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the Internet Web site page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person's or business's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(k) For purposes of this section, "encryption key" and "security credential" mean the confidential key or process designed to render data useable, readable, and decipherable.

(*l*) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Credits

(Added by Stats.2002, c. 1054 (A.B.700), § 4, operative July 1, 2003. Amended by Stats.2007, c. 699 (A.B.1298), § 6; Stats.2011, c. 197 (S.B.24), § 2; Stats.2013, c. 396 (S.B.46), § 2; Stats.2014, c. 855 (A.B.1710), § 2, eff. Jan. 1, 2015; Stats.2015, c. 522 (A.B.964), § 2, eff. Jan. 1, 2016; Stats.2015, c. 532 (S.B.34), § 2, eff. Jan. 1, 2016; Stats.2015, c. 543 (S.B.570), § 2.3, eff. Jan. 1, 2016; Stats.2016, c. 86 (S.B.1171), § 21, eff. Jan. 1, 2017; Stats.2016, c. 337 (A.B.2828), § 2, eff. Jan. 1, 2017.)

Notes of Decisions (5)

Footnotes

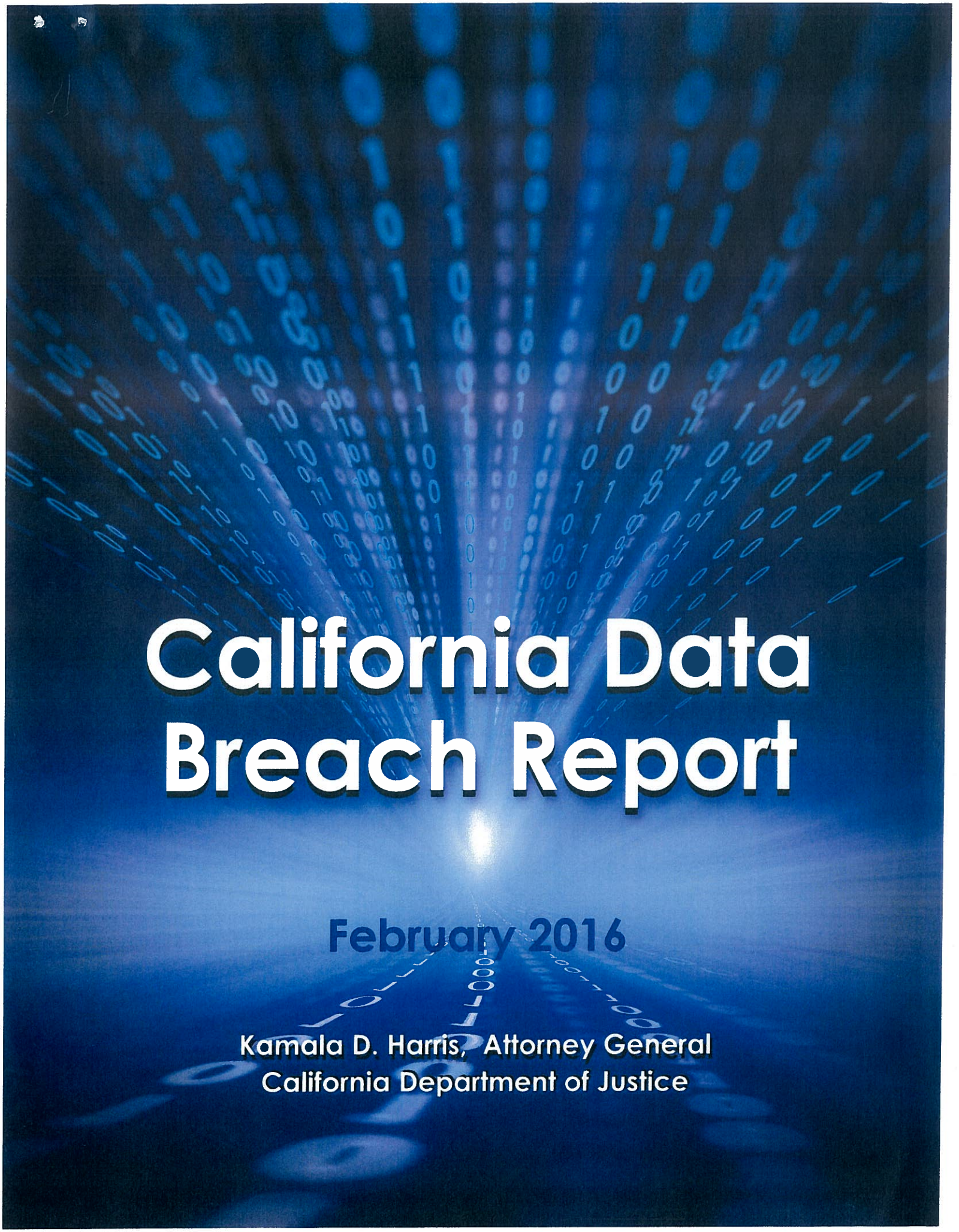
1 For public law sections classified to the U.S.C.A., see USCA-Tables.

West's Ann. Cal. Civ. Code § 1798.82, CA CIVIL § 1798.82

Current with all 2016 Reg.Sess. laws, Ch. 8 of 2015-2016 2nd Ex.Sess., and all propositions on 2016 ballot.

End of Document

Exhibit "5"


California Data
Breach Report
February 2016
Kamala D. Harris, Attorney General
California Department of Justice

Message from the Attorney General

The California Constitution guarantees every Californian the "inalienable right" to privacy. To ensure that protection, California has been on the cutting edge, adopting the strongest and most sophisticated consumer privacy laws in the United States. But California's fast-changing economy requires our constant vigilance to ensure that privacy and security protections keep pace with innovation and new threats. Each day, millions of Californians log on to the internet to conduct business, do homework, purchase goods and services, control devices in their homes, play games, and connect with loved ones. Technology such as smartphones, the "internet of things," wearable devices, and big data are transforming our lives at a rapid pace, while exponentially increasing the amount of personal information that is collected, used, and shared. At the same time, with data becoming more ubiquitous and valuable, the black market for stolen information also continues to expand, increasing the likelihood of hacking by cyber criminals.

With more of our personal information online, it is imperative that organizations employ strong privacy practices. To protect privacy, businesses must have privacy policies that are easy to read and access, inform consumers about material changes to their data handling practices, and carefully select their default settings which often determine how data is collected, used, and shared. Foundational to those privacy practices is information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access.

Data breaches, particularly when they involve sensitive information such as Social Security numbers and health records, threaten not only the privacy but also the security and economic wellbeing of consumers. Breaches also impact a wide range of industries, from the health care and financial services sectors to retail and small businesses, and pose a threat to critical infrastructure and national security. Now that organizations rely increasingly on the collection and use of personal information and criminals take advantage of security weaknesses to obtain and profit from that same information, it is more important than ever that all of us redouble our efforts to ensure that this data does not end up in the wrong hands.

The report that follows provides a comprehensive analysis of the data breaches reported to my office from 2012 to 2015. In the last four years, nearly 50 million records of Californians have been breached and the majority of these breaches resulted from security failures.

Furthermore, nearly all of the exploited vulnerabilities, which enabled these breaches, were compromised more than a year after the solution to patch the vulnerability was publicly available. It is clear that many organizations need to sharpen their security skills, trainings, practices, and procedures to properly protect consumers.

Securing data is no doubt challenging, with sophisticated cyber criminals – including some nation states – waging an escalating battle. But many of the breaches reported to us could have been prevented by taking reasonable security measures, and an organization that voluntarily chooses to collect and retain personal information takes on a legal obligation to adopt appropriate security controls.

As we become further immersed in the online world, our lives and our livelihoods depend more and more on our ability to use technology securely. The potential of a digitally connected society is immense, so it is critical that we put the appropriate safeguards in place before individuals feel that they must either abandon their right to privacy or go offline to protect it. This report is a starting point, and a call to action, for all of us—organizations, individuals, and regulators—to work toward a safer and more secure online future.

Sincerely,

Attorney General Kamala D. Harris