William Mitchell Law Review

Volume 39 | Issue 4 Article 9

2013

The Spam Filter Ate My E-Mail: When Are Electronic Records Received

Jevon C. Bindman

THE SPAM FILTER ATE MY E-MAIL: WHEN ARE ELECTRONIC RECORDS RECEIVED?

Jevon C. Bindman†

† JD Candidate, William Mitchell College of Law, May 2014; MM, Choral Conducting, Michigan State University, 2007; BA cum laude, Music, Cornell University, 2005. I would like to thank Professor Christina L. Kunz (William Mitchell College of Law) for her invaluable guidance throughout. Thanks also to Professor D. Benjamin Beard, Michael Fleming, Michael J. McGuire, Thomas J. Smedinghoff, and R. David Whitaker for providing essential background and analysis. Finally, thank you to my wife, Jancyn, who gives meaning to everything I do.

I. INTRODUCTION

Awaiting Acceptance: You have just made an offer to sell fifty sofas to a furniture store. The store manager says he will e-mail his acceptance later that day. Your e-mail system's third-party spam filter, which inspects messages before they enter your system, is somewhat overactive. Through no fault of the store manager, the filter deletes the message and you never see it.[1]

Rotten Recall: A television company is conducting a voluntary recall of one of its most popular models. The company sends you an e-mail recall notice. In order to ensure that the notice will reach as few customers as possible, the company intentionally doctors the e-mail to include large fonts and colorful text. The e-mail enters your system and your spam filter intercepts it. The e-mail is routed to your junk mail folder and you never see it.[2]

Flower Fanatic: You are a member of a flower gardening interest group called "flowers-r-us." Members send gardening tips to each other through e-mail. These messages say "flowers-r-us" in the subject line. Since you receive numerous "flowers-r-us" e-mails each day, you create a rule on your computer to route all such e-mails to a "gardening" folder, which you check infrequently. One day, you see an interesting tip on how to care for hydrangeas, and you forward the e-mail to a business associate. The associate replies, "Great article! By the way, I've attached a new offer for the contract we've been working on." Since "flowers-r-us" is still included in the subject line, the reply e-mail gets routed to the gardening folder and you never read it.[3]

The Uniform Electronic Transactions Act (UETA) defines when an electronic message is "sent" and "received."[4] However,

1. *See* Dean N. Alterman, *Guess What Your Spam Filter Just Bought for You*, PORTLAND BUS. J. (Apr. 4, 2004, 9:00 PM), http://www.bizjournals.com/portland/stories/2004/04/05/focus5.

2. *See* Cem Kaner, *SPAM, Filtering, and Commercial Legislation*, CEM KANER, J.D., PH.D. (May 1, 2003, 5:53 AM), http://kaner.com/?p=25.

3. This hypothetical is adapted from an interview with Michael J. McGuire, Chief Info. Sec. Officer, Littler Mendelson, in St. Paul, Minn. (Sept. 10, 2012).

4. *See* UETA § 15(a), (b) (1999).

several issues emerge upon application of these definitions to situations like the hypotheticals above.[5] Is a message received if it is intercepted by an overactive filter, or is the sender out of luck? Does it matter whether the recipient's spam filter is located inside or outside of the recipient's server? Should it matter who manages the recipient's spam filter—the recipient, the system manager, or a third-party contractor? Does a recipient have recourse when a message is intercepted by a spam filter due to the sender's negligent or sharp practices? One court has suggested a draconian solution:

> In defending their failure to [acknowledge the court's e-mail notice], the appellants offer nothing but an updated version of the classic "my dog ate my homework" line. . . . Imperfect technology may make a better scapegoat than the family dog in today's world, but not so here. Their counsel's effort at explanation, even taken at face value, is plainly unacceptable.[6]

This note, however, will argue that the solution is not so cut-and-dry. Part II will briefly chronicle the rise of electronic communication and the laws that govern it and will highlight the similarities and differences between the laws' definitions of "send" and "receive."[7] Part III will review the development of spam filters and illustrate the uncertainties that arise when spam filters interact with UETA's definitions of "send" and "receive."[8]

Part IV will explore three partial and concurrent solutions to the spam filter issue: (1) a rebuttable presumption that a properly sent record is received, (2) use of the consumer-protection provision in the Electronic Signatures in Global and National Commerce Act (E-SIGN) to provide insulation from sharp business practices, and (3) a test that allocates responsibility to both sender and recipient according to the factors that each party controls.[9] The note will conclude by arguing that, since both sender and recipient benefit from the use of electronic communication, both parties should share the responsibility of preventing messages from being intercepted by spam filters.[10]

5. *See generally* Thomas J. Smedinghoff, *Electronic Document Delivery and the Problem of Spam Filters*, 4 PRIVACY & SECURITY L. REP. 301 (2005).
6. Fox v. Am. Airlines, Inc., 389 F.3d 1291, 1294 (D.C. Cir. 2004).
7. *See infra* Part II.
8. *See infra* Part III.
9. *See infra* Part IV.
10. *See infra* Part V.

II. HISTORY OF ELECTRONIC COMMUNICATION LAWS

A. Rise in Electronic Communication

In the late 1960s, businesses began to develop electronic data interchange (EDI), which allowed them to communicate electronically with standardized purchase orders, invoices, and other documents.[11] This new technology resulted in fewer transmission errors, lowered transaction costs, better customer service, and improved cash flow.[12] By 1991, EDI was used by 15,000 companies worldwide.[13] As EDI fundamentally changed the way contracts for the sale of goods were entered into and performed, proponents realized that existing law (including common law and the UCC) potentially made those electronic documents legally unenforceable.[14]

The ABA Electronic Messaging Services Task Force wrote the EDI Model Trading Partners Agreement ("EDI Model Agreement") to dispel these concerns.[15] The EDI Model Agreement sought to "assur[e] the validity and predictability of the related commercial [EDI] transactions" and included the first definition of an electronic writing.[16] Drafters knew, however, that the EDI Model Agreement was only a "first step" and recommended "the development of an ongoing comprehensive strategy to accomplish appropriate legal reform."[17]

The earliest electronic communication laws in the United States diverged widely at the state level.[18] Some state statutes were technology-specific, while others were media-neutral; some were narrow in scope, while others were broad.[19] Some states combined these approaches while others did nothing at all.[20] A sharp rise in

11. Elec. Messaging Servs. Task Force, Am. Bar Ass'n., *The Commercial Use of Electronic Data Interchange—A Report and Model Trading Partner Agreement*, 45 BUS. LAW. 1645, 1649 (1990); Christina L. Kunz, *The Definitional Hub of E-commerce: "Record,"* 45 IDAHO L. REV. 399, 401 (1999).

12. Kunz, *supra* note 11, at 401.

13. *Id.*

14. Elec. Messaging Servs. Task Force, Am. Bar Ass'n., *supra* note 11, at 1649–50.

15. *See generally id.*

16. Kunz, *supra* note 11, at 403–04.

17. Elec. Messaging Servs. Task Force, Am. Bar Ass'n., *supra* note 11, at 1647.

18. *See* Robert A. Wittie & Jane K. Winn, *Electronic Records and Signatures Under the Federal E-SIGN Legislation and the UETA*, 56 BUS. LAW. 293, 294–96 (2000).

19. *Id.* at 295–96.

20. *Id.*

the use of electronic communication, combined with the lack of uniformity in state statutes, created the need for uniform laws to facilitate and encourage electronic commerce, validate electronic transactions, and foster uniformity.[21]

B. Scope of Electronic Communication Laws

The following chart briefly summarizes the scope and adoption of the relevant electronic communication laws that have been drafted since 1996: the U.N. Model Law on Electronic Commerce ("Model Law"), UETA, the Uniform Computer Information Transactions Act (UCITA), E-SIGN, and the U.N. Convention on the Use of Electronic Communications in International Contracts ("Convention").[22]

21. *See* UETA § 6; UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT, at 30, U.N. Doc. A/51/162, U.N. Sales No. E.99.V.4 (1999) [hereinafter UNCITRAL].

22. For more information, see 2 IAN C. BALLON, E-COMMERCE AND INTERNET LAW § 15.01 (2d ed. 2011); DOCUMENTING E-COMMERCE TRANSACTIONS §§ 2:2, 3:2, 4:1 (William A. Hancock ed., 2011).

	Model Law (1996)	*UETA (1999)*	*UCITA (1999)*	*E-SIGN (2000)*	*Convention (2005)*
Drafter	U.N. Commission on International Trade Law (UNCITRAL)	National Conference of Commissioners on Uniform State Laws (NCCUSL)[23]	NCCUSL	Congress	UNCITRAL
Where Adopted	Provides a framework for national legislation[24]	Forty-seven states, D.C., and U.S. Virgin Islands[25]	Maryland and Virginia[26]	United States	Countries where Convention is ratified[27]
Scope of Covered Transactions	*Model Law art. 1*: Commercial activity	*UETA § 5(b)*: Parties agreeing to communicate electronically[28]	*UCITA § 103*: Computer Information	*15 U.S.C. § 7001(a)*: Interstate or foreign commerce[29]	*Convention art. 1, para. 1*: Parties located in different countries
Notable Exclusions	None, but limiting language is suggested in Model Law article one	*UETA § 3(b)*: Wills and trusts, UCITA, UCC (except Article Two)	*UCITA § 103(d)*: Exclusions are extensive	*15 U.S.C. § 7003(a)*: Wills, trusts, family law, UCC (except Article Two)	*Convention art. 2, para. 1*: Consumer transactions

Each electronic communication law defines what "writings" are within its scope. UETA defines a "record" as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."[30] An "electronic record" is "a record created, generated, sent, communicated, received, or stored by electronic means."[31] This definition is nearly identical to those found in the Model Law,

23. NCCUSL is now known as the Uniform Law Commission (ULC).

24. UNCITRAL, *supra* note 21, at 16–17.

25. *See* UETA Refs. & Annots. (West, Westlaw through 2011 annual meetings) (excluding Illinois, New York, and Washington).

26. BALLON, *supra* note 22, § 15.03[1]. Four states have enacted statutes to prevent UCITA from governing a contract entered into by their citizens. *See id.*

27. Ratification has been limited. *See Status 2005—United Nations Convention on the Use of Electronic Communications in International Contracts*, UNCITRAL, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html (last visited Feb. 19, 2013).

28. Such agreements are determined by context and should be broadly construed (e.g., ordering goods online or including an e-mail address on a business card). UETA § 5(b), cmt. 4 (1999).

29. Congress intends for E-SIGN to apply broadly. Adam R. Smart, *E-SIGN Versus State Electronic Signature Laws: The Electronic Statutory Battleground*, 5 N.C. BANKING INST. 485, 492 n.46 (2001).

30. UETA § 2(13).

31. *Id.* § 2(7).

UCITA, E-SIGN, and the Convention.[32] It intends to encompass all types of electronic information, including those arising from "foreseeable technical developments."[33] Similarly, the laws consistently define an "information processing system" as "an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information."[34]

C. Relevant Provisions of Electronic Communication Laws

The main thrust of the electronic communication laws discussed above is that an electronic record or signature may not be denied legal effect solely because it is in an electronic form.[35] In other words, the difference between an electronic and paper record is irrelevant in judging the legal validity of a document.[36] The laws also provide requirements regarding accuracy of an original document,[37] attribution,[38] and retention capability.[39] They do not, however, require electronic records to be used,[40] nor do they establish the legal validity of an electronic record[41]—that

32. *See* 15 U.S.C. § 7006(4) (2006) (defining "electronic record"); United Nations Convention on the Use of Electronic Communications in International Contracts, G.A. Res. 60/21, art. 4(c), U.N. Doc. A/RES/60/21 (Nov. 23, 2005) [hereinafter Convention] (defining "data message"); Model Law on Electronic Commerce, G.A. Res. 51/162, art. 2(a), U.N. Doc. A/RES/51/162 (Dec. 16, 1996) [hereinafter Model Law] (same); UCITA § 102(a)(26), (55) (2002) (defining "electronic" and "record").

33. *See* UNCITRAL, *supra* note 21, at 23–24, 26.

34. UETA § 2(11); *see* Convention, *supra* note 32, art. 4(f) (defining "information system"); Model Law, *supra* note 32, art. 2(f) (same); UCITA § 102(36) (2002) (defining "information processing system"). Although E-SIGN does not provide a definition of "system," UETA's definition applies in states that have enacted UETA. *See infra* text accompanying notes 58–60.

35. *See* 15 U.S.C. § 7001(a); Convention, *supra* note 32, art. 8, para. 1; Model Law, *supra* note 32, art. 5; UCITA § 107; UETA § 7.

36. UETA § 7 cmt. 1; *see also* U.N. COMM'N ON INT'L TRADE LAW, UNITED NATIONS CONVENTION ON THE USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS, at 47, U.N. Doc. A/Res/60/21, U.N. Sales No. E.07.V.2 (2007) [hereinafter UNCITRAL] ("[E]lectronic communications [will] achieve the same degree of legal certainty as paper-based communications.").

37. 15 U.S.C. § 7001(d)(1); Model Law, *supra* note 32, art. 8; UETA § 12(a).

38. Model Law, *supra* note 32, art. 13; UETA § 9.

39. 15 U.S.C. § 7001(d); Model Law, *supra* note 32, art. 10; UETA § 12.

40. 15 U.S.C. § 7001(b)(2); UNCITRAL, *supra* note 21, at 30 ("[T]he Model Law . . . should not be construed in any way as imposing [the use of electronic means of communication]."); UETA § 5(a).

41. UETA Refs. & Annots. Prefatory Note B (West, Westlaw through 2011 annual meetings); UNCITRAL, *supra* note 21, at 32; *see* BALLON, *supra* note 22, § 15.02[2][A] ("[E-SIGN] generally does not alter substantive contract law.").

determination is left to the applicable area of substantive law.[42]

The electronic communication laws also define when electronic records are sent and received.[43] UETA provides:

> (a) [A]n electronic record is sent when it:
>
> (1) is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;
>
> (2) is in a form capable of being processed by that system; and
>
> (3) enters an information processing system outside the control of the sender . . . or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient.[44]

A message is addressed or directed properly to a recipient when there is "specific information which will direct the record to the intended recipient."[45] Subsection (a)(3) provides that an electronic record is sent when it leaves the sender's system or, if the message never leaves the sender's system, when the record is under the recipient's control (i.e., when the record is received).[46]

The UETA definition of "receipt" is essentially a subset of its definition of "sent" because a received message has necessarily been sent.[47] It provides:

> (b) [A]n electronic record is received when:
>
> (1) it enters an information processing system that the recipient has designated or uses for the purpose of

42. UETA employs a "minimalist approach" to ensure solely that electronic records are "treated in the same manner . . . as written records." UETA Refs. & Annots. Prefatory Note (Westlaw). Similarly, the goal of the Model Law is to create a "media-neutral environment." UNCITRAL, *supra* note 21, at 17.

43. *See* Model Law, *supra* note 32, art. 15; UETA § 15. These provisions may be varied by agreement. *See* Model Law, *supra* note 32, art. 15 (stating that the definition applies "[u]nless otherwise agreed"); UETA § 15 (same).

44. UETA § 15(a); *see also* Convention, *supra* note 32, art. 10, para. 1 (defining "dispatch"); Model Law, *supra* note 32, art. 15, para. 1 (same).

45. UETA § 15 cmt. 2. This definition covers mass mailings but not "general broadcast message[s], sent to systems rather than individuals . . . ." *Id.*

46. *Id.* § 15(a)(3) & cmt. 2. For example, employees of the same university or corporation may share the same system. *Id.* § 15 cmt. 2. In such a situation, sending and receipt are simultaneous. UNCITRAL, *supra* note 21, at 55.

47. R. David Whitaker, *An Overview of Some Rules and Principles for Delivering Consumer Disclosures Electronically*, 7 N.C. BANKING INST. 11, 21 (2003); *see* UETA § 15(a), (b).

> receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and
>
> (2) it is in a form capable of being processed by that system. . . .
>
> . . . .
>
> (e) An electronic record is received . . . even if no individual is aware of its receipt.[48]

Subsection (b)(1) defines receipt as the time that an electronic record is capable of being retrieved, as opposed to when the message is accessible or actually viewed.[49] If receipt were otherwise defined, a recipient could effectively block receipt by not accessing or viewing the record.[50] Additionally, it is impractical for the sender to prove not only that a record was received but that it was also accessed or viewed.[51] Since e-mail protocol cannot provide automatic acknowledgment of receipt,[52] such proof would require a recipient's manual acknowledgment, which the recipient could easily falsify (and could require acknowledgment of the acknowledgment, etc.).[53]

Subsection (e) notes that an electronic record may be received before the recipient has read it or even knows of its existence.[54] Up until the 1999 NCCUSL Annual Meeting, the UETA draft also

48. UETA § 15(b), (e); *see also* Model Law, *supra* note 32, art. 15, para. 2 (defining "receipt").

49. UETA § 15(b)(1); *see* Elec. Messaging Servs. Task Force, Am. Bar Ass'n., *supra* note 11, at 1732 (stating that a message is received under the EDI Model Agreement when it is "accessible to the receiving party").

50. *See* Richard A. Lord, *A Primer on Electronic Contracting and Transactions in North Carolina*, 30 CAMPBELL L. REV. 7, 62 (2007) ("[T]he recipient is foreclosed from arguing that he did not receive the information simply because he did not access it . . . ."); *cf.* Henk Snijders, *The Moment of Effectiveness of E-mail Notices*, *in* E-COMMERCE LAW 79, 80 (Henk Snijders & Stephen Weatherill eds., 2003) (arguing in favor of a receipt rule similar to that in UETA).

51. Snijders, *supra* note 50, at 80.

52. Telephone Interview with Michael Fleming, Senior Corporate Counsel, Cray, Inc. (Sept. 21, 2012). The current standard e-mail protocol, RFC-5321, is based on an e-mail protocol written in 1989. *Id.*; *see Simple Mail Transfer Protocol*, INTERNET ENGINEERING TASK FORCE (Oct. 2008), http://tools.ietf.org/html/rfc5321.

53. Telephone Interview with Michael Fleming, *supra* note 52; *cf.* CHRISTINA L. KUNZ & CAROL L. CHOMSKY, CONTRACTS: A CONTEMPORARY APPROACH 343 (2010) (discussing the same concept regarding the mailbox rule). The EDI Model Agreement does require verification of receipt. Elec. Messaging Servs. Task Force, Am. Bar Ass'n., *supra* note 11, at 1667.

54. UETA § 15 cmt. 5. The paper equivalent is an unread letter in a mailbox. *Id.*

stated that an electronic record was *effective* upon receipt, rejecting the common law mailbox rule.[55] Although UCITA retains this provision,[56] the UETA Drafting Committee decided not to alter substantive contract law in an effort to preserve media neutrality and avoid bad policy.[57]

While E-SIGN does not contain sending and receiving rules, UETA's definitions still apply in states where it is enacted.[58] E-SIGN does not preempt UETA when a state enacts the official version of UETA or enacts a similar law that is consistent with E-SIGN and does not grant preferred status to a certain technology used for creating electronic records.[59] If the state-enacted legislation is exempted from preemption and E-SIGN does not contain a comparable provision, then the UETA provision applies.[60] Therefore, UETA's send and receipt rules apply, notwithstanding E-SIGN, in states that have enacted the official UETA or a similar law.[61]

The 2005 Convention modifies the definition of "receipt" in two ways.[62] Unlike UETA and the Model Law, which define receipt as the time that the record enters the recipient's system, a record is not received under the Convention until it is "capable of being retrieved by the [recipient]."[63] However, UNCITRAL did not intend this language to demonstrate a modification from the

55. NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS, DRAFT FOR APPROVAL: UNIFORM ELECTRONIC TRANSACTIONS ACT § 114(e) & n.5 (1999), *available at* http://www.uniformlaws.org/shared/docs/electronic%20transactions/etaam.pdf.

56. *See* UCITA § 214(a), cmt. 2 (2002) ("Subsection (a) . . . reject[s] the mailbox rule for electronic messages . . . .").

57. Amelia H. Boss, *The Uniform Electronic Transactions Act in a Global Environment*, 37 IDAHO L. REV. 275, 335 (2001).

58. *See* 15 U.S.C. § 7002(a) (2006).

59. *Id.*

60. *See id.* (allowing state law to "modify, limit, or supersede" E-SIGN); Shea C. Meehan & D. Benjamin Beard, *What Hath Congress Wrought: E-sign, the UETA, and the Question of Preemption*, 37 IDAHO L. REV. 389, 406 (2001) ("[W]here the UETA has provisions with no analog in E-sign . . . , the UETA will apply.").

61. A state enactment of UETA likely need not be a "pristine" version of the official UETA in order to be exempted from preemption. *See* Meehan & Beard, *supra* note 60, at 403–04 (finding that a requirement of a pristine adoption could cause "absurd results").

62. *See* Convention, *supra* note 32, art. 10.

63. *Id.* art. 10, para. 2. *Compare* Model Law, *supra* note 32, art. 15, para. 2 (enters a "designated information system"), *and* UETA § 15(b)(1) (1999) (enters an "information processing system"), *with* Convention, *supra* note 32, art. 10, para. 2. The time at which an electronic record is capable of retrieval is "left for the applicable law." UNCITRAL, *supra* note 36, at 61.

Model Law receipt requirements.[64] The Convention also includes a presumption that a record is "capable of being retrieved by the [recipient] when it reaches the [recipient]'s electronic address."[65] This presumption "may be rebutted by evidence showing that the [recipient] had in fact no means of retrieving the communication."[66]

III. SPAM FILTERS AND THEIR INTERACTION WITH UETA

A. Spam—Definition and Early Prevention Efforts

Spam is most broadly defined as "[u]nsolicited commercial e-mail."[67] In November 2012, an estimated sixty-three percent of e-mail was spam.[68] There are three types of spam: messages sent by legitimate marketers who are concerned with customer privacy, messages that "employ quasi-legal methods" to recruit as many customers as possible, and "traditional" spam sent by malicious software that converts computers into "botnets" to relay potentially harmful messages.[69]

In an effort to curb the disruption caused by spam, as well as its toll on the economy,[70] Congress enacted the Controlling the

64. *See* UNCITRAL, *supra* note 36, at 61–62 ("[T]he rules on receipt of electronic [records] in the . . . Convention [are] consistent with article 15 of the UNCITRAL Model Law . . . .").

65. Convention, *supra* note 32, art. 10, para. 2. There is no substantive difference between "electronic address" and "information system." UNCITRAL, *supra* note 36, at 62.

66. UNCITRAL, *supra* note 36, at 62 (citation omitted). In 2009, the ULC considered amending UETA to mirror the Convention's presumption requirement. *See* Henry D. Gabriel & D. Benjamin Beard, *2009 Annual Meeting Report*, UNIFORM L. COMMISSION 2 (May 29, 2009), http://www.uniformlaws.org/Committee.aspx?title=UN%20E-Commerce%20Convention (follow "2009 Annual Meeting Report, Exhibit D" hyperlink). Instead, the ULC urged Congress to ratify the Convention (which Congress has not done). *Id.* at 1 (follow "2009 Annual Meeting Report" hyperlink).

67. BLACK'S LAW DICTIONARY 1524 (9th ed. 2009); *see also* David Lorentz, *The Effectiveness of Litigation Under the CAN-SPAM Act*, 30 REV. LITIG. 559, 562 (2011) ("[N]either the courts nor any secondary sources have provided a consistent definition of 'spam.'").

68. Darya Gudkova, *Spam in November 2012*, SECURELIST (Dec. 19, 2012), http://www.securelist.com/en/analysis/204792258.

69. *See* Lorentz, *supra* note 67, at 564–67; Kara Rowland, *Clever Spammers Stay 'One Step Ahead' of Law*, WASH. TIMES, Dec. 6, 2006, at A1.

70. *See* Jonathan Krim, *Spam's Cost to Business Escalates*; *Bulk E-mail Threatens Communication Arteries*, WASH. POST, Mar. 13, 2003, at A1 (estimating that spam would cost U.S. organizations over $10 billion in 2003).

Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act") in 2003.[71] Among its goals were to reduce the amount of spam received in inboxes, increase the convenience of e-mail communication, discourage the sending of "vulgar" materials, and prevent spammers from misleading spam recipients.[72] The CAN-SPAM Act prohibits the sending of false, misleading, or deceptive information;[73] requires the inclusion of a functioning return e-mail address;[74] and requires the sender to provide an opportunity for the recipient to "opt-out" of receiving future messages.[75] It is unclear as to whether the CAN-SPAM Act has effected a decrease in the amount of spam received by e-mail users.[76] Some critics argue that, while the Act successfully curbs the spamming practices of "legitimate" companies, those companies make up only a small percentage of the spamming population.[77] Others contend that Congress's intent was to "legalize legitimate, unsolicited e-marketing" rather than decrease the amount of spam received.[78] Regardless, spam has continued to pose a major threat to e-mail security and e-commerce.[79]

B. Advent of Spam Filters

An excessive amount of spam, coupled with the lack of effective legislation, necessitated the creation of spam filtering programs.[80] In general, a spam filter reduces the amount of spam received by filtering out messages that appear to be spam.[81] When

71. 15 U.S.C. §§ 7701–13 (2006).
72. *Id.* § 7701.
73. *Id.* § 7704(a)(1), (2).
74. *Id.* § 7704(a)(3).
75. *Id.* § 7704(a)(5).
76. *Compare* FED. TRADE COMM'N, EFFECTIVENESS AND ENFORCEMENT OF THE CAN-SPAM ACT 7 (2005), *available at* http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf (noting a decrease in spam), *with* John Soma et al., *Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions*, 45 HARV. J. ON LEGIS. 165, 165 (2008) (noting an increase in spam).
77. Rowland, *supra* note 69.
78. Lorentz, *supra* note 67, at 576; *see also* Matthew E. Shames, Note, *Congress Opts Out of Canning Spam*, 66 U. PITT. L. REV. 385, 403 (2004) (noting that Congress did not want to restrict all spam, as e-mail "is an inexpensive way for businesses to advertise their products" (quoting 149 CONG. REC. S13,125 (daily ed. Oct. 23, 2003) (statement of Sen. Feingold))).
79. *See* Smedinghoff, *supra* note 5 ("[S]pam . . . threatens to render e-mail useless as a means of communication.").
80. *See id.* ("One very promising solution is spam filtering.").
81. *See* L. Elizabeth Bowles et al., Am. Bar Ass'n, *Program Materials:*

a filter identifies a message as spam, it deletes the message or "quarantines" it into a junk mail folder.[82] Spam filters typically block messages based on the sender's domain name (e.g., "@wmitchell.edu") and the message's content.[83]

Spam filters block e-mails sent from specific domain names by relying on realtime blackhole lists (RBLs).[84] RBLs are maintained by third-party list generators, who can be either for-profit companies or "good Samaritans."[85] When the RBL generator suspects a domain name of sending spam, the domain is "blacklisted" by inclusion on the RBL. Additionally, some RBL generators maintain a list of server relays that spammers frequently use.[86] Spam filters purchase RBLs and block the domains and servers included on the lists.[87]

Although RBLs greatly reduce the amount of spam that ends up in a user's inbox, they may block legitimate e-mails as well.[88] Since the lists are compiled in part from individual complaints, RBLs can be inaccurate.[89] An RBL can blacklist a domain merely because the domain's server allows spamming activity.[90] Further, a legitimate domain may have difficulty getting removed from the list and may have to pay a fee.[91]

Second, spam filters examine a message's content by searching for phrases, words, and layouts that "look[] like spam."[92] Each

Technological Controls on Spam and Their Legal Implications, LARKIN HOFFMAN 5 (Apr. 2005), http://www.larkinhoffman.com/files/OTHER/47.pdf.

82. Smedinghoff, *supra* note 5.

83. *See How Does the Spam Filter Work?*, U. PENN. ENGINEERING, http://www.seas.upenn.edu/cets/answers/spamblock-filter.html (last visited Feb. 20, 2013).

84. *Id.* For more information on RBLs, see SPAMHAUS, http://www.spamhaus.org (last visited Feb. 20, 2013).

85. Interview with Michael J. McGuire, *supra* note 3.

86. Carla Schroder, *Realtime Black-Hole Lists: Heroic Spam Fighters or Crazed Vigilantes?*, ENTERPRISE NETWORKING PLANET (Feb. 24, 2003), http://www.enterprisenetworkingplanet.com/netsysm/article.php/1594561/.

87. A small minority of spam filters instead use "whitelists," which allow e-mail only from the domains included on the list. Bowles et al., *supra* note 81, at 7. This method results in fewer spam messages but requires significant upkeep on the part of the recipient to keep the whitelist current. *Id.*

88. *See* Schroder, *supra* note 86 (demonstrating that a spam-friendly server can result in the blocking of all domains using that server).

89. Bowles et al., *supra* note 81, at 6.

90. *See* Schroder, *supra* note 86 (asserting that some RBLs block "both spammers and open relays").

91. *See* Bowles et al., *supra* note 81, at 6; *see also SBL Delisting Procedure*, SPAMHAUS, http://www.spamhaus.org/sbl/delistingprocedure/ (last visited Feb. 20, 2013) (outlining procedures for removal from a Spamhaus RBL).

92. *How Does the Spam Filter Work?*, *supra* note 83. For example, the filter may

instance of an irregular word or phrase increases the message's "spam score."[93] Once the score is high enough, the message is filtered.[94] Like RBLs, content filters may be influenced by users.[95]

Content filters require a great deal of upkeep.[96] Spamming trends change over time to reflect world events, so the words and phrases used in spam will change accordingly.[97] In addition, a spammer will frequently change her approach in an attempt to "beat" the spam filter.[98] Due to the specific advantages and disadvantages of RBL and content filters, most spam filters use a combination of domain-based and content-based blockers.[99]

A message is likely to pass through numerous filters on its journey from sender to recipient.[100] First, the sender's system may filter the message to protect against outbound spam and to prevent the release of sensitive information.[101] Next, the message will likely pass through several "relay" servers, each of which may have its own filter system.[102] Upon arrival at the recipient's system, a message may pass through a filter maintained by the system manager or by a third-party agent of the manager.[103] These filters may be located outside or within the recipient's system.[104] Finally, the recipient's individual workstation is likely to apply a final round of filters.[105]

Despite attempts to intercept only illegitimate or harmful

search for words like "Viagra" or layouts such as large fonts and blinking lights. *Id.*

93. Bowles et al., *supra* note 81, at 8–9. For an example of the various tests employed by spam filters, see *What Headers Are Added to E-mails That Are Scanned by SpamAssassin?*, LAMP HOST, http://www.lamphost.com/node/82 (last visited Feb. 20, 2013).

94. Bowles et al., *supra* note 81, at 9.

95. *See, e.g.*, *So Much Time, So Little Spam*, GOOGLE, http://mail.google.com/intl/ar/mail/help/fightspam/spamexplained.html (last visited Feb. 20, 2013) ("When the Gmail community . . . report[s] a particular email as spam, our system . . . block[s] similar messages.").

96. *See* Bowles et al., *supra* note 81, at 10 ("The rules need to be constantly updated . . . .").

97. *See* Gudkova, *supra* note 68 (noting that, in November 2012, a considerable amount of spam referenced Hurricane Sandy and the upcoming holiday season).

98. *See* Rowland, *supra* note 69 (noting that spammers have learned how to "throw off filter keyword searches").

99. *See* Bowles et al., *supra* note 81, at 6, 8–10 (noting the advantages and disadvantages of each filtering method).

100. Interview with Michael J. McGuire, *supra* note 3.

101. *Id.*

102. *Id.*

103. *Id.*

104. *Id.*

105. *Id.*

messages, spam filters nevertheless intercept some legitimate messages as well. In an informal survey conducted by the author,[106] twenty-five percent of respondents found one or more personal e-mails (i.e., a message intended for the recipient alone) in their junk e-mail folder. Eighty-one percent of respondents found one or more commercial e-mail (i.e., a mass-produced e-mail sent to many recipients) to which they had subscribed.[107]

C. Interaction Between Spam Filters and UETA

Spam filters were not on the radar of the UETA Drafting Committee.[108] Although spam is believed to have been invented in the mid-1990s,[109] it did not become a major concern until the mid-2000s.[110] Consequently, UETA was drafted and enacted without attention to spam filters, and the interaction between UETA and spam filters has become a source of contention among experts in electronic communication laws and among states that have enacted UETA.[111] Businesses have been forced to accept the deluge of spam

106. Survey questions are available at *Spam and Junk Mail Survey*, SURVEYMONKEY, http://www.surveymonkey.com/s/9HDHCGG (last visited Feb. 20, 2013).

107. Respondents reported that 5% of the e-mails in the junk mail folder were personal e-mails, 32% were commercial e-mails, and 62% were spam.

108. Telephone Interview with D. Benjamin Beard, Reporter, UETA Drafting Comm. (Sept. 14, 2012); Telephone Interview with Thomas J. Smedinghoff, Am. Bar Ass'n Advisor, UETA Drafting Comm. (asserting that the Committee was more concerned with the "time and place" of delivery than the "fact" of delivery). *But see* Kaner, *supra* note 2 (asserting that the Committee did consider spam filters).

109. Credence E. Fogo, *The Postman Always Rings 4,000 Times: New Approaches to Curb Spam*, 18 J. MARSHALL J. COMPUTER & INFO. L. 915, 915–16 (2000) (claiming that spam was invented by two lawyers seeking to advertise their services).

110. Jonathan Krim, *FTC Files Suit Against Sender of Porn 'Spam,'* WASH. POST, Apr. 18, 2003, at E1 (noting that spam represented 8% of all e-mail traffic in 2001 and 40% in 2003).

111. *See, e.g.*, Assembly Comm. on Judiciary, *AB 328 Bill Analysis*, CAL. LEGIS. INFO. 8 (May 5, 2009), http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab_0301-0350/ab_328_cfa_20090504_125946_asm_comm.html (opposing a bill that would allow insurance companies to send notifications electronically); Smedinghoff, *supra* note 5 ("If . . . the message is quarantined or deleted by a spam filter, has the sender failed to . . . deliver information, or has the recipient assumed the risk?"); Soma et al., *supra* note 76, at 169 ("When legitimate e-mails are accidentally filtered, potentially important communications are lost."); Bowles et al., *supra* note 81, at 5 ("[T]he fact that legitimate e-mail may be blocked by these increasingly effective filters . . . mean[s] that your life . . . promises to become a lot more uncertain . . . ."); Gail Hillebrand, *Uniform Electronic Transactions Act: Consumer Nightmare or Opportunity?*, CONSUMERS UNION (Aug. 23, 1999), http://www.consumersunion.org/finance/899nclcwc.htm ("A message is received

or install spam filters, knowing that some legitimate e-mail will likely be blocked as well.[112] These issues are likely to become more significant as e-commerce continues to develop because more communication will come under the purview of UETA.[113]

The growing use of new technologies, such as messaging through cell phones and social networks, makes spam filter issues an even more pressing concern.[114] These technologies are quickly replacing e-mail as the preferred method of communication,[115] but they lack the relative stability of e-mail systems.[116] While most e-mail servers retain a copy of e-mails that enter or leave the system,[117] most cell phone carriers do not retain text message content.[118] Although carriers do retain text message details (such as the name of the sender and the date and time of dispatch), some new messaging systems—such as Apple's iMessage—circumvent the carriers, making documentation even more uncertain.[119] Spammers have already become more active in soliciting cell phone users.[120] As spam filters become more commonplace in new technologies,[121] they will likely encounter many of the same issues that currently exist with e-mail; therefore, the interaction between

even . . . when the message was automatically discarded by a junk mail filter.").

112. *See Filters Cut Off E-mail That Businesses Want*, WASH. TIMES (Feb. 22, 2004), http://www.washingtontimes.com/news/2004/feb/22/20040222-103456-4989r/ ("Many companies forgo paying for filters to block unwanted e-mail, fearing that legitimate messages will be blocked.").

113. *See* UETA § 5(b) (1999); *see also supra* note 28 & accompanying text.

114. *See* UETA § 2 cmt. 4 (advocating an expansive definition of "electronic" so that UETA "will be applied broadly as new technologies develop").

115. *See* Sarah Radwanick, *The 2010 U.S. Digital Year in Review*, COMSCORE 10–11, 28 (Feb. 7, 2011), http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/2010_US_Digital_Year_in_Review (follow "Download Whitepaper" hyperlink) (noting a decrease in e-mail use and an increase in messaging through social network and text message use in most age groups).

116. Interview with Michael J. McGuire, *supra* note 3.

117. *See IMAP & POP*, U. MINN., http://www.oit.umn.edu/email/imap-pop/index.htm (last modified June 11, 2012) (demonstrating that modern e-mail systems retain copies of messages on the server unless deleted by the recipient).

118. *See Retention Periods of Major Cellular Service Providers*, A.C.L.U., http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart (last visited Feb. 20, 2013).

119. *See* Jenna Wortham, *Free Texts Pose Threat to Carriers*, N.Y. TIMES, Oct. 10, 2011, at B1.

120. *See* Nicole Perlroth, *Spam Invades a Last Refuge, the Cellphone*, N.Y. TIMES, Apr. 8, 2012, at A1 (noting a steep rise in text message spamming since 2009).

121. *See* Eric A. Taub, *Eluding a Barrage of Spam Text Messages*, N.Y. TIMES, Apr. 5, 2012, at A9 (presenting a variety of spam filter tools provided by cell phone carriers).

UETA and new technologies may pose an even greater problem than the current e-mail issues.

IV. SOLUTIONS FOR DETERMINING IF A RECORD HAS BEEN RECEIVED

This section will explore three partial and concurrent solutions for determining whether a filtered electronic record has been sent and received: (1) a rebuttable presumption that a message is received when it is properly sent or when it enters the recipient's system,[122] (2) use of the consumer protection provisions in E-SIGN,[123] and (3) a test that accounts for the sender's and recipient's ability to prevent a spam filter from intercepting an electronic record.[124]

A. Rebuttable Presumption of Receipt

1. Presumption in General

Presumption of receipt of paper mail has long existed in American common law.[125] Courts universally hold that a letter that is properly directed and dispatched is presumed to have been received by the recipient.[126] Rather than a "conclusive presumption of law," the presumption is an "inference of fact" that the postal service will properly deliver the letter.[127] Consequently, the presumption may be rebutted by evidence that the letter was not received, and the factfinder makes the final determination by weighing the evidence brought by the sender and recipient.[128]

The policy underlying the presumption of receipt is addressed

122. *See infra* Part IV.A.
123. *See infra* Part IV.B.
124. *See infra* Part IV.C.
125. *E.g.*, Rosenthal v. Walker, 111 U.S. 185, 193–94 (1884); Grade v. Mariposa Cnty., 64 P. 117, 117–18 (Cal. 1901); Pitts v. Hartford Life & Annuity Ins. Co., 34 A. 95, 97 (Conn. 1895); Hamilton v. Stewart, 34 S.E. 123, 125 (Ga. 1899); Ashley Wire Co. v. Ill. Steel Co., 45 N.E. 410, 413 (Ill. 1896); Huntley v. Whittier, 105 Mass. 391, 392–93 (1870); Plath v. Minn. Farmers' Mut. Fire Ins. Ass'n, 23 Minn. 479, 484–85 (1877); Austin v. Holland, 69 N.Y. 571, 576 (1877).
126. *E.g.*, *Rosenthal*, 11 U.S. at 193; *accord Pitts*, 34 A. at 97; *Hamilton*, 34 S.E. at 125; *Huntley*, 105 Mass. at 392; *Austin*, 69 N.Y. at 576. While the presumption is often referred to as the "mailbox rule," this author refrains from that term so as to avoid confusion with the mailbox rule as applied to acceptance of an offer. *See* RESTATEMENT (SECOND) OF CONTRACTS § 63 (1981) ("[A]n acceptance . . . is operative . . . as soon as put out of the offeree's possession . . . .").
127. *Rosenthal*, 11 U.S. at 193; *Huntley*, 105 Mass. at 392–93.
128. *Rosenthal*, 11 U.S. at 193–94; *Huntley*, 105 Mass. at 392–93.

in *Ashley Wire Co. v. Illinois Steel Co.*:

> The presumption that the letter was received is founded upon the regularity and certainty with which the mail is carried and delivered. When letters are properly stamped and addressed, the uniformity with which they are received is such that the failure to receive such letter is a very unusual circumstance . . . .[129]

The presumption is further strengthened by the fact that postal workers "are charged by law with the proper delivery of the mail, and are presumed to have performed those duties in a proper manner."[130]

Courts have generally held that a positive and uncontradicted denial of receipt is sufficient for a factfinder to determine that a presumption of receipt has been rebutted.[131] However, courts tend to support a presumption of receipt when the recipient's rebuttal is less than a categorical denial of receipt[132] or when the sender contradicts the rebuttal with evidence that the letter likely was received.[133] Regardless of whether the presumption of receipt is met or rebutted, most courts hold that the burden of proving receipt remains with the sender.[134]

Presumption of receipt of e-mails has not been applied as uniformly and universally as it has for paper mail.[135] On one hand, the Eighth Circuit has held that the presumption should apply to "other forms of communication—such as . . . electronic mail . . . —

129. *Ashley*, 45 N.E. at 413.

130. Smedinghoff, *supra* note 5.

131. *See, e.g.*, Planters' Mut. Ins. Ass'n v. Green, 80 S.W. 151, 151 (Ark. 1904); Grade v. Mariposa Cnty., 64 P. 117, 118 (Cal. 1901); Hill v. Wiles, 92 A. 996, 996–97 (Me. 1915). *But see In re* Alexander's, Inc., 176 B.R. 715, 721 (Bankr. S.D.N.Y. 1995) ("[T]he addressee must do more than simply deny that it received notice."). A line of Georgia cases has held that an uncontradicted denial of receipt by the recipient may overcome the presumption *as a matter of law*. *See, e.g.*, *Hamilton*, 34 S.E. at 125.

132. *See, e.g.*, W.E. Richmond & Co. v. Sec. Nat'l Bank, 64 S.W.2d 863, 869 (Tenn. Ct. App. 1933) (holding the presumption not overcome when the recipient does not remember whether he received the letter or when another company member may have received it).

133. *See, e.g.*, Jensen v. McCorkell, 26 A. 366, 367 (Pa. 1893) (finding that the presence of the sender's return address strengthened the presumption of receipt).

134. Huntley v. Whittier, 105 Mass. 391, 392–93 (1870) ("[T]he burden of proving . . . receipt remains throughout upon the party who asserts it."); *see also* Travelers' Ins. Co. of Hartford, Conn. v. Farmers' Mut. Fire Ins. Ass'n of Monona Cnty., 233 N.W. 153, 156 (Iowa 1930) ("[T]he burden of [proving receipt] is nevertheless upon the [sender].").

135. BALLON, *supra* note 22, § 14.05[3].

provided they are accepted as generally reliable . . . ."[136] When determining whether the presumption was properly rebutted, courts have considered whether the notice was intercepted by a spam filter,[137] sent improperly due to a computer glitch,[138] or accessed on a different computer,[139] as well as whether the sender received a "bounce-back" message[140] or the recipient has demonstrated a "lack of diligence."[141]

However, this line of cases has been limited solely to presuming receipt of notice of an electronic court filing (ECF).[142] Thus far, courts have not determined whether a presumption of receipt exists for other e-mail and messaging systems.[143] Even if a court recognizes a presumption of receipt, it may require different types of proof than those required for paper mail.[144]

2. Disadvantages of a Rebuttable Presumption of Receipt

Two different presumptions have been suggested as a solution to the interaction between spam filters and UETA's definition of "send" and "receive." The "strong" presumption is that an electronic record should be presumed received when it is properly sent.[145] The "weak" presumption is that a record should be

136. Am. Boat Co. v. Unknown Sunken Barge (*Am. Boat Co. I*), 418 F.3d 910, 914 (8th Cir. 2005) (citation omitted).

137. Am. Boat Co. v. Unknown Sunken Barge (*Am. Boat Co. II*), 567 F.3d 348, 353 (8th Cir. 2009); *see also* Pace v. AIG, Inc., No. 8 C 945, 2010 WL 4530357, at *1, *3 (N.D. Ill. Nov. 1, 2010) (finding "excusable neglect" due in part to spam filter excuse); *In re* Philbert, 340 B.R. 886, 890 (Bankr. N.D. Ind. 2006) (rejecting spam filter excuse); Tobin v. Granite Gaming Grp. II, L.L.C., No. 2:07-CV-577-BES-PAL, 2008 WL 723337, at *10 (D. Nev. Mar. 17, 2008) (same).

138. *Am. Boat Co. II*, 567 F.3d at 353.

139. *Id.*

140. *Id.*

141. *See Pace*, 2010 WL 4530357, at *2 ("Unlike here, the cases cited . . . involve situations where an attorney's malfunctioning e-mail is just one example of the attorney's overall lack of diligence.").

142. *See Am. Boat Co. I*, 418 F.3d 910, 914 (8th Cir. 2005); Dempster v. Dempster, 404 F. Supp. 2d 445, 449 (E.D.N.Y. 2005).

143. *Cf.* BALLON, *supra* note 22, §14.05[3] ("In many cases . . . the presumption of receipt should not necessarily apply merely because a communication was sent.").

144. *See* SSI Med. Servs., Inc. v. State Dept. of Human Servs., 685 A.2d 1, 6 n.1 (N.J. 1996); *see also* BALLON, *supra* note 22, § 14.05[3] ("Not all of the assumptions underlying . . . evidentiary presumptions on terra firma . . . necessarily hold true online.").

145. *See, e.g.*, OR. REV. STAT. ANN. § 84.072(4) (West, Westlaw through 2012 Reg. Sess.) ("A notice sent . . . to an electronic mail address . . . is presumed to have been received . . . ."); *Am. Boat Co. I*, 418 F.3d at 913 ("If [the court's ECF]

presumed received when it enters the recipient's system.[146] Proponents argue that a rebuttable presumption is necessary as a safeguard for the recipient.[147] They assert that, since e-mail is less reliable than paper mail,[148] a recipient should have an avenue for disputing receipt when a message is intercepted by a spam filter or otherwise fails to reach its destination.[149] A rebuttable presumption would allow the recipient to present evidence that a spam filter intercepted the record.[150]

First, as a matter of statutory interpretation, the plain language of UETA does not support a presumption of receipt.[151] Under the "strong" presumption that a properly sent message is received, "the real issue is whether the sender properly mailed the notice, not

entries indicated that an e-mail was sent and not returned as undeliverable, then receipt of that e-mail would be presumed."); Letter from Cem Kaner, Attorney at Law, to Donald S. Clark, Sec'y, Fed. Trade Comm'n (Apr. 30, 1990), http://www.ftc.gov/bcp/icpw/comments/kaner.htm ("[T]he [UETA] receipt rule should involve a presumption . . . [and] the intended recipient should be able to rebut the presumption of receipt . . . ."). *But see* CAL. R. CT. 2.259(a)(4) (West, Westlaw through Dec. 15, 2012) ("In the absence of the court's confirmation of receipt and filing, there is no presumption that the court received and filed the document.").

146. Convention, *supra* note 32, art. 10, para. 2 ("An electronic communication is presumed to be capable of being retrieved by the [recipient] when it reaches the [recipient]'s electronic address."); UNIFORM ELECTRONIC COMMERCE ACT, para. 23(2) (1999) (Can.), *available at* http://www.ulcc.ca/en/uniform-acts-en-gb-1/298-electronic-commerce-act/74-electronic-commerce-act?showall=&start=2 ("An electronic document is presumed to be received by the addressee, (a) when it enters an information system designated or used by the addressee . . . ."); *see* Smedinghoff, *supra* note 5 ("The UNCITRAL [Convention] approach may well be a good first step toward addressing the spam filter problem.").

147. *See* Letter from Cem Kaner to Donald S. Clark, *supra* note 145 ("A rule that states that e-mail is received when it [enters the recipient's system] subjects the recipient to risk . . . .").

148. *See* Boss, *supra* note 57, at 336 n.299 (noting that one out of ten e-mails fails to reach its destination); Letter from Cem Kaner to Donald S. Clark, *supra* note 145 ("[E-mail providers] have no tradition of reliable delivery and no liability if they fail to deliver e-mail.").

149. *See* UNCITRAL, *supra* note 36, at 61; Letter from Cem Kaner to Donald S. Clark, *supra* note 145 ("The intended recipient should be able to rebut the presumption of receipt.").

150. *See Am. Boat Co. I*, 418 F.3d at 914 (ordering an evidentiary hearing to determine whether the presumption was rebutted); UNCITRAL, *supra* note 36, at 62; Letter from Cem Kaner to Donald S. Clark, *supra* note 145 (providing examples of facts sufficient to rebut presumption of receipt).

151. *See* Lord, *supra* note 50, at 58–59; *see also* Boss, *supra* note 57, at 336–37 & n.307 ("The question remains . . . of how to prove or even presume receipt."); Smedinghoff, *supra* note 5 (arguing that UETA contains no presumption of receipt because it seeks to determine the "'time' of receipt").

whether the intended recipient received it."[152] If this presumption were adopted, UETA's "receipt" provisions would be surplusage because any properly sent message would be presumed received.[153] The "weak" presumption, which presumes a message to be received when it enters the recipient's system, is similarly unsupported by UETA.[154] UETA plainly states that a message *is* received when it enters the recipient's system; once the message reaches that point, therefore, the presumption is meaningless.[155] Further, UETA does not provide substantive rules of law; it serves only to validate electronic records.[156] Thus, it would be inappropriate to "read in" a presumption of receipt.[157]

Second, the relative unreliability of e-mail[158] makes inadvisable a presumption of receipt. The presumption of receipt of paper mail grew out of the tremendous reliability of the postal system, making it extremely unlikely that a properly dispatched letter would fail to be received.[159] Consequently, the presumption benefits the sender when receipt is disputed.[160] In contrast, an electronic record can encounter countless issues on its journey from sender to recipient.[161] Given this unreliability, a presumption of receipt would provide the sender an undeserved benefit.[162]

While courts have touted the reliability of e-mail in their decisions to support a presumption of receipt, these decisions have

152. *In re* Schepps Food Stores, Inc., 152 B.R. 136, 139 (Bankr. S.D. Tex. 1993).

153. *See Id.* at 139–40; UETA § 15(b) (1999).

154. *See, e.g.*, Convention, *supra* note 32, art. 10, para. 2.

155. *See* UETA § 15(b).

156. UETA Refs. & Annots. Prefatory Note (West, Westlaw through 2011 annual meetings) ("[T]he substantive rules of contracts remain unaffected by UETA.").

157. *See* Lord, *supra* note 50, at 58–59.

158. *See supra* note 148.

159. *See* Ashley Wire Co. v. Ill. Steel Co., 45 N.E. 410, 413 (Ill. 1896).

160. *See, e.g.*, 57 THOMAS J. CZELUSTA ET AL., NEW YORK JURISPRUDENCE 2D EVIDENCE AND WITNESSES § 139 (2012), *available at* Westlaw NYJUR EVIDENCE ("[A] failure to show that the letter was correctly addressed will *deprive the sender of the benefit of such presumption*." (emphasis added)).

161. *See supra* text accompanying notes 100–105. See *Email Delivery Problems Explained*, TOP WEB HOSTS, http://www.topwebhosts.org/articles/email-delivery-problems.php (last visited Feb. 20, 2013), for a list of potential e-mail delivery problems.

162. Telephone Interview with R. David Whitaker, Counsel, Buckley Sandler LLP (Sept. 17, 2012) (all opinions, conclusions, or recommendations expressed are those of Mr. Whitaker and do not necessarily reflect the views of Buckley Sandler LLP).

been limited to receipt of ECF notices.[163] ECF systems are likely more reliable than commercial e-mail systems because they are less likely to have delivery problems.[164] Further, the court receives a "bounce-back" message when an ECF notice fails to reach the recipient's system.[165] Finally, attorneys have a duty to monitor the docket, making ECF notices a mere convenience.[166] For these reasons, a court is unlikely to lend the same level of deference to a commercial e-mail system; however, a court could be justified in applying a presumption if a messaging system is as reliable as ECF.[167]

In conclusion, a rebuttable presumption does provide the recipient an opportunity to dispute receipt. However, a presumption is inadvisable because it opposes the plain language of UETA and ignores the relative unreliability of e- mail.

B. E-SIGN Consumer Protection Provisions

1. General Requirements and Limited Scope

Next, this note will explore whether the E-SIGN consumer disclosure provision provides protection to consumers when a message sent by a business is intercepted by a spam filter.[168] Unlike the Model Law and UETA, which apply generally to consumers without any consumer-specific rules,[169] E-SIGN provides specific

163. *See, e.g.*, Am. Boat Co. v. Unknown Sunken Barge (*Am. Boat Co. I*), 418 F.3d 910, 914 (8th Cir. 2005); Dempster v. Dempster, 404 F. Supp. 2d 445, 449 (E.D.N.Y. 2005).

164. Am. Boat Co. v. Unknown Sunken Barge (*Am. Boat Co. II*), 567 F.3d 348, 351 (8th Cir. 2009) ("The district court's CM/ECF administrator . . . testified that the system had never experienced a glitch . . . [and that he had] '100 percent' confidence that the Notice was received by [the attorney's system].").

165. *See id.*; Moore v. United States, No. S 04-0423 FCD JFM, 2005 WL 1984745, at *3 (E.D. Cal. Aug. 17, 2005), *rev'd on other grounds*, 262 F. App'x 828 (9th Cir. 2008).

166. Fox v. Am. Airlines, Inc., 389 F.3d 1291, 1294 (D.C. Cir. 2004) ("Regardless whether [the attorney] received the e-mail notice, he remained obligated to monitor the court's docket."); *see also Moore*, 2005 WL 1984745, at *5 ("[The attorney] did not make an effort to obtain those communications through [the online docket] . . . .").

167. *Cf., e.g.*, Kunz, *supra* note 11, at 400 (describing the "dedicated modem connections" of EDI communications).

168. "'[C]onsumer' means an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes . . . ." 15 U.S.C. § 7006(1) (2006).

169. *See* UETA § 3 legis. n.4 (1999); UNCITRAL, *supra* note 21, at 24–25 ("[T]here [is] no reason why situations involving consumers should be excluded

consumer protection.[170] It should be noted, however, that this provision has a limited scope.[171] Obviously, it protects only consumers; in addition, it applies only to records sent *to* consumers, not records sent *by* them.[172] Further, E-SIGN mandates consumer consent only when notice in writing is legally required by state or federal law.[173] Written notice is not legally required in most situations, including situations involving contract formation.[174]

The E-SIGN consumer protection provision sets up redundant procedures to ensure that the consumer has consented to receiving electronic records and that the records can be reliably received.[175] In transactions governed by E-SIGN, any notice for which a writing is legally required may not be provided electronically until the consumer "has affirmatively consented to such use."[176] Among other requirements, the consumer must be provided a "clear and conspicuous statement" explaining the hardware and software requirements for accessing and retaining the records, the consumer's right to obtain the record in paper form, and the procedure for withdrawing consent.[177] After receiving this statement, the consumer must provide electronic consent in a way that demonstrates she can access the electronic documents.[178] Unless these requirements are met, an electronic record does not satisfy a business's legal obligation to provide information to a consumer in writing.[179]

Subsection (c)(1)(D) outlines situations in which the entity providing notice must reaffirm consent:

from the scope of the Model Law . . . .").

170. *See* 15 U.S.C. § 7001(c).

171. *See* Wittie & Winn, *supra* note 18, at 303–05 ("[T]he consumer consent provisions apply in limited circumstances.").

172. *Id.* at 304; *see* 15 U.S.C. § 7001(c)(1) (protecting electronic records "provided or made available to a consumer").

173. Wittie & Winn, *supra* note 18, at 304; *see* 15 U.S.C. § 7001(c)(1).

174. Wittie & Winn, *supra* note 18, at 304. In fact, even after a contract has been formed, lack of E-SIGN consent to receive records electronically does not invalidate that contract. DOCUMENTING E-COMMERCE TRANSACTIONS, *supra* note 22, § 4:3; *see* 15 U.S.C. § 7001(c)(3).

175. BALLON, *supra* note 22, § 15.02[2][C].

176. 15 U.S.C. § 7001(c)(1)(A).

177. *Id.* § 7001(c)(1)(B)–(C).

178. *Id.* § 7001(c)(1)(C)(ii). Electronic consent or confirmation can be achieved by any means that "reasonably demonstrates" consent to accept electronic records. *Id.* For a list of best practices in obtaining electronic consent, see DOCUMENTING E-COMMERCE TRANSACTIONS, *supra* note 22, § 4:3.

179. *See* 15 U.S.C. § 7001(c)(1).

> [A]fter the consent of a consumer [has been obtained], if a *change in the hardware or software requirements* needed to access or retain electronic records creates a *material risk* that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record [must]—
>
> (i) provide[] the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent . . . ; and
>
> (ii) again compl[y] with [the consent requirements described above].[180]

Based on this provision, a business may be required to notify a consumer when its e-mail practices create a risk that a message will be intercepted by a spam filter. However, two ambiguities in the provision make this conclusion uncertain. First, what spam practices could constitute a "change in the hardware or software requirements needed to access . . . a subsequent electronic record"?[181] Second, what spam practices could constitute a "material risk" that the record will not be received?[182]

2. "Change in Requirements" and "Material Risk"

When Congress debated E-SIGN in 2000, it anticipated that changes in technology would necessitate changes in the way electronic records are sent and received.[183] For example, a business may undergo a system upgrade to implement newly installed hardware.[184] A particular web browser may no longer be supported by the sender's or recipient's system.[185] In essence, the redisclosure requirement could apply to *any* change, no matter how trivial, in the hardware and software requirements needed for the recipient to receive the sender's message.[186]

180. *Id.* § 7001(c)(1)(D) (emphasis added).
181. *See id.*
182. *See id.*
183. *See* Robert A. Cook et al., *The Electronic Signatures in Global and National Commerce Act—A Review of the Act's Consumer Disclosure Requirements*, 54 CONSUMER FIN. L.Q. REP. 315, 322 (2000).
184. *See* BALLON, *supra* note 22, § 15.02[2][C].
185. *See, e.g.*, *Supported Browsers*, GMAIL, support.google.com/mail/bin/answer.py?hl=en&answer=6557 (last visited Feb. 20, 2013).
186. Telephone Interview with R. David Whitaker, *supra* note 162.

However, too broad of an interpretation could burden e-commerce[187] and annoy consumers who would be inundated by redisclosure notifications.[188] Congress sought to protect consumer interests while limiting the burden on e-commerce.[189] Therefore, E-SIGN was written to require redisclosure only when changes in hardware or software requirements pose a "material risk" to receipt by the consumer.[190]

Congress did not, however, provide what constitutes a material risk. A fact is material when "knowledge of the item would affect a person's decision-making."[191] Therefore, a change in hardware or software requirements is material, requiring redisclosure under E-SIGN, when knowledge of the change would affect the recipient's decision to accept documents electronically.

Some changes in required hardware or software would almost certainly not affect a recipient's decision to continue receiving electronic documents. For example, the release of a new version of a web browser does not create a material risk because upgrades are readily available.[192] In fact, many electronic disclosure agreements state that only the most recent version of a web browser is supported.[193] Conversely, a change may be material if the sender decides to no longer support *any* version of a popular web browser.[194]

There are several business practices concerning spam filters that likely constitute material risks. For example, a recipient's

187. *See* Wittie & Winn, *supra* note 18, at 307 ("[The E-SIGN consumer consent provisions] place a high compliance burden on businesses.").

188. *See id.* ("[C]onsumers . . . will need to wade through lengthy and perhaps repetitive consent forms in order to do business electronically.").

189. *See* 15 U.S.C. § 7005(b) (2006) (authorizing an evaluation of the burdens that E-SIGN imposes on e-commerce); Cook et al., *supra* note 183, at 316 (asserting that Congress sought to provide consumer protections while limiting burdens to e-commerce); *see also* Fed. Trade Comm'n & Dep't of Commerce, *E-SIGN: The Consumer Consent Provision in Section 101(c)(1)(C)(ii)*, FED. TRADE COMMISSION (June 2001), http://www.ftc.gov/os/2001/06/esign7.htm (reporting on the benefits and burdens that E-SIGN imposes on e-commerce).

190. 15 U.S.C. § 7001(c)(1)(D).

191. *E.g.*, Huston v. Procter & Gamble Paper Prods. Corp., 568 F.3d 100, 107 (3d Cir. 2009) (quoting BLACKS' LAW DICTIONARY 998 (8th ed. 2004)); *In re* AFI Holding, Inc., 530 F.3d 832, 846 (9th Cir. 2008) (same).

192. Telephone Interview with R. David Whitaker, *supra* note 162; *see, e.g.*, *Internet Explorer 9 Delivery Through Automatic Updates*, MICROSOFT, http://technet.microsoft.com/en-us/ie/gg615599.aspx (last visited Feb. 20, 2013).

193. Telephone Interview with R. David Whitaker, *supra* note 162.

194. *See, e.g.*, The Associated Press, *AOL to End Support of Netscape Navigator*, N.Y. TIMES, Dec. 29, 2007, at C8.

decision to accept electronic documents would certainly be affected if the sender increased the "spam score" of its electronic records[195] or used a server relay that is listed on several RBLs.[196] It is less clear whether a recipient's decision would be affected if the sender begins to send more bulk e-mails.[197]

Statements from congressional debates confirm that E-SIGN intends to place the burden of consent requirements on the sender:

> Most individuals lack the technological sophistication to know the exact technical specifications of their computer equipment and software. It is appropriate to require companies to establish an "electronic connection" with their customers in order to provide assurance that the consumer will be able to access the information in the electronic form in which it will be sent.[198]

One could argue that this "electronic connection" is severed when a sender acts in a way that greatly increases the chance of its electronic records being intercepted by a spam filter. It is likely, therefore, that a sender who does so is required to reestablish consent from the consumer.

In conclusion, while the E-SIGN consumer disclosure provision may provide consumer protection from businesses engaged in negligent or sharp practices, its limited scope makes it inapplicable in a majority of situations.

C. Accountability Test

The third spam filter solution accounts for each party's ability to prevent a spam filter from intercepting an electronic record. It holds the sender responsible if its message is likely to be intercepted by a spam filter, and it holds the recipient responsible if the recipient maintains an unreasonable spam filter or fails to check for filtered messages in a junk mail folder.[199] Rather than

195. *See supra* text accompanying notes 92–95.

196. *See supra* text accompanying notes 84–87.

197. A sender of bulk e-mails is more likely to be included on an RBL. Telephone Interview with Michael Fleming, *supra* note 52.

198. 146 CONG. REC. S5230 (daily ed. June 15, 2000) (statement of Sens. Hollings, Wyden, & Sarbanes); *see also* 146 CONG. REC. H4360 (daily ed. June 14, 2000) (statement of Rep. Tauzin) ("[T]he provisions regarding consent afford consumers with the greatest possible safeguards against fraud imaginable.").

199. *Cf.* Smedinghoff, *supra* note 5 ("If the intended recipient does not receive a message because the message is quarantined or deleted by a spam filter,

creating a "bright-line rule," this test is necessarily fact-specific.[200] For example, while the term "Viagra" is likely to raise the spam score of a message,[201] that term may be appropriate if the sender is a pharmaceutical company.

Late-nineteenth- and early-twentieth-century cases involving mistaken telegraph transmissions provide historical support for the accountability test. These cases generally stated that a telegram recipient could not be held accountable for acting upon an erroneous message when there was no reason for the recipient to doubt the accuracy of the message,[202] even if the telegram contradicted previous correspondence.[203] The telegraph test was fact-specific: the recipient could not be penalized for relying on a message that "was not unintelligible . . . [or] couched in extraordinary or unusual language."[204] If, however, the recipient acted on a message that he should reasonably have known contained errors, then the recipient was held accountable for any negative effect.[205]

UETA uses a similar test to determine the effect of an error in transmission.[206] If both parties have agreed to use a security procedure to detect errors in transmission, and an error occurs due to one party's failure to conform to the procedure, the conforming party can avoid any negative effect caused by the error.[207] The

has the sender failed to fulfill a legal obligation to deliver information, or has the recipient assumed the risk?").

200. *See* Campbell v. Gen. Dynamics Gov't Sys. Corp., 407 F.3d 546, 554 (1st Cir. 2005) (using a "fact-dependent" test to determine whether appropriate notice was given); Reece v. Wal-Mart Stores, Inc., 98 F.3d 839, 843 (5th Cir. 1996) (declining to establish a "bright-line rule" regarding who is authorized to receive service of process), *abrogated in part by* Murphy Bros., Inc. v. Michetti Pipe Stringing, Inc., 526 U.S. 344 (1999).

201. *See* Bowles et al., *supra* note 81, at 9.

202. *See, e.g.*, McCarty v. W. Union Tel. Co., 91 S.W. 976, 977 (Mo. Ct. App. 1906); W. Union Tel. Co. v. Beals, 76 N.W. 903, 905 (Neb. 1898); W. Union Tel. Co. v. Edsall, 12 S.W. 41, 43 (Tex. 1889).

203. *See* Henry v. W. Union. Tel. Co., 131 P. 812, 813 (Wash. 1913) (holding that the recipient could reasonably have assumed that his purchasing agent had been successful in reducing the offer).

204. *Beals*, 76 N.W. at 905.

205. *See, e.g.*, W. Union Tel. Co. v. Wright, 18 Ill. App. 337, 340 (1885) (finding the recipient contributorily negligent for acting on an erroneous telegram after being informed of the mistake); Hart v. Direct U.S. Cable Co., 86 N.Y. 633, 633–34 (1881) (holding that the recipient "took the risk" of interpreting a message that contained "unintelligible jargon").

206. *See* UETA § 10 (1999).

207. *Id.* § 10(1).

provision "operates against the non-conforming party, i.e., *the party in the best position to have avoided the change or error*, regardless of whether that person is the sender or recipient."[208] Similarly, the accountability test seeks to hold responsible the party in the best position to avoid interception by a spam filter.[209]

The following sections will examine the factors controlled by the sender and the recipient and argue that each party should be responsible for the consequences of its actions concerning those factors.

1. Factors Controlled by the Sender

The sender has control over the content and dispatch of an electronic record. As shown above, the sender's deliberate, reckless, or negligent actions can affect whether a message is likely to be intercepted by a spam filter.[210] If a message is filtered before entering the recipient's system, the sender's actions are inconsequential because the message has failed to be received anyway.[211] But what if the message is filtered *after* it enters the recipient's system? According to the language of UETA, it would appear that the message was received and the recipient "assumed the risk" of using a spam filter.[212] However, two UETA provisions may potentially protect a recipient from a sender's sharp or negligent practices. First, an electronic record must be "addressed properly."[213] Second, the record must be "in a form capable of being processed" by the recipient's system.[214]

a. "Addressed Properly"

First, an electronic record must be "addressed properly" or "otherwise directed properly" to the recipient's system.[215] The message must contain "specific information which will direct the

208. *Id.* § 10 cmt. 2 (emphasis added).
209. *See id.*
210. *See supra* notes 84–87 & 92–95.
211. UETA § 15(b). *But see infra* Part IV.C.2 (suggesting a broader definition of the recipient's system).
212. Smedinghoff, *supra* note 5, at 2; *see also* UETA § 15(b) (stating that an electronic record is received when it enters the recipient's processing system).
213. UETA § 15(a)(1).
214. *Id.* § 15(a)(2). An electronic record must also be "in a form capable of being processed" at the time of receipt. *Id.* § 15(b)(2).
215. *Id.* § 15(a)(1).

record to the intended recipient."[216] An improperly addressed message has not been sent.[217] Although a message may be received even if not properly sent,[218] an improper address affects receipt because the message is less likely to enter the recipient's system and the recipient is less likely to be "able to retrieve the electronic record."[219]

Obviously, the sender has not properly addressed a message in which the recipient's electronic address is incorrect.[220] In addition, a message may not be properly addressed when the sender's electronic practices increase the likelihood of the sender being "blacklisted," because inclusion on an RBL greatly decreases the chance that the message will be "direct[ed] . . . to the intended recipient."[221] Several factors affect a sender's likelihood of being blacklisted, including the reputation of the sender's domain name and the reputation of the system or server relays used by the sender.[222] If sending messages in bulk, a sender is more likely to be blacklisted if the recipient list is "opt-out" rather than "opt-in"[223] or if the sender fails to include an "opt-out" statement.[224]

While courts have not published opinions on what constitutes a "properly addressed" *electronic* record under UETA, ample case law exists relating to *paper* records:

> [A] "proper" address would be "characterized by appropriateness or suitability" for its intended purpose. The purpose of an address is to supply information for delivery of mail to its intended destination. Hence, an address containing errors inconsequential to delivery is still proper.
>
> . . . Where an address, *ex ante*, enables delivery to the intended destination, then that address is proper and any

216. *Id.* § 15 cmt. 2. Mass sending, as in the case of bulk messages, is covered as long as the messages are sent to individuals rather than as a "general broadcast message." *Id.*

217. *Id.* § 15(a).

218. *See id.* § 15(b) (not requiring proper dispatch as a precursor to receipt).

219. *Id.* § 15(b)(1).

220. *See id.* § 15(a)(1) (requiring that the sender direct the message to a system designated by the recipient or a system used by the recipient for similar messages).

221. Telephone Interview with Michael Fleming, *supra* note 52; *see* UETA § 15(a)(1), cmt. 2.

222. Telephone Interview with Michael Fleming, *supra* note 52.

223. RBLs tend to be more skeptical of "opt-out" lists because the recipient has not affirmatively consented to being included on the list. *Id.*

224. *Id.*

error is inconsequential.[225]

An error is inconsequential when it is "so minor that it would not prevent delivery of the notice."[226] Thus, an address is improper if an error would cause a message to fail to reach its destination.[227]

Using this definition, courts have generally held that an incorrect zip code is an inconsequential error and does not result in an improper address.[228] A zip code "facilitate[s] the delivery" of mail but is not a necessary part of the address.[229] If the letter contains the correct name and address, an incorrect zip code is unlikely to prevent delivery or cause delay, especially when the error is minor.[230] In contrast, a letter with an incorrect address *and* zip code is improperly addressed.[231]

Blacklisting factors are more similar to an incorrect name or address than an incorrect zip code. While an incorrect zip code usually is inconsequential and a mere inconvenience to postal workers,[232] blacklisting factors are more than inconvenient because they can prevent a message from being delivered at all.[233] An absence of blacklisting factors is a necessary part of the sender's message and does more than merely "facilitate the delivery."[234]

Therefore, a recipient may be protected from a sender's sharp or negligent practices if the sender engages in blacklisting factors

225. Santoro v. Principi, 274 F.3d 1366, 1370 (Fed. Cir. 2001) (citation omitted); *see, e.g.*, Busquets-Ivars v. Ashcroft, 333 F.3d 1008, 1010 (9th Cir. 2003) (determining whether a piece of mail was "properly directed"); Judkins v. Davenport, 59 S.W.3d 689, 690–91 (Tex. App. 2000) (same).

226. Pickering v. Comm'r, 75 T.C.M. (CCH) 2152, at *2 (1998).

227. *See Santoro*, 274 F.3d at 1370; *Pickering*, 75 T.C.M. (CCH) 2152, at *2.

228. *See, e.g.*, Price v. Comm'r, 76 T.C. 389, 392–93 (1981); *Judkins*, 59 S.W.3d at 691. *But see Busquets-Ivars*, 333 F.3d at 1010 ("The INS fails to [properly send the letter] because the zip code used was incorrect.").

229. *Judkins*, 59 S.W.3d at 691; *see Pickering*, 75 T.C.M. (CCH) 2152, at *2 ("[T]he ZIP code number . . . is for the convenience of the Postal Service and is helpful to ensure prompt delivery." (quoting Watkins v. Comm'r, 63 T.C.M. (CCH) 1710 (1992))); *Price*, 76 T.C. at 392 ("The use of zip codes is for the convenience of the Postal Service . . . .").

230. *Pickering*, 75 T.C.M. (CCH) 2152, at *3 (unlikely to prevent delivery); Smetanka v. Comm'r, 74 T.C. 715, 719 (1980) (unlikely to cause delay).

231. Int'l Television Film Prod., Inc. v. Comm'r, 45 T.C.M. (CCH) 1049, 1049 (1983).

232. *See Pickering*, 75 T.C.M. (CCH) 2152, at *2 ("[T]he ZIP code number . . . is for the convenience of the Postal Service . . . ." (quoting *Watkins*, 63 T.C.M. (CCH) at 1710 (1992))).

233. *Id.*; *see also* Santoro v. Principi, 274 F.3d 1366, 1370 (Fed. Cir. 2001) ("Where an address . . . enables delivery to the intended destination, then that address is proper and any error is inconsequential.").

234. *See Judkins*, 59 S.W.3d at 691.

that cause the message to be improperly addressed. In that case, the sender should be responsible for nonreceipt because the sender was in the best position to prevent the filter from intercepting the message.

b. "Form Capable of Being Processed"

Second, an electronic record must be "in a form capable of being processed by [the recipient's] system" at the time of sending and at the time of receipt.[235] While UETA does not address the legal effectiveness of electronic records,[236] this provision implicitly involves the content of the message. The sender has sole control over the content of the message. Specifically, she has the ability to avoid practices that would tend to raise the message's "spam score."[237] If a message has a high spam score, it may not be "in a form capable of being processed" by the recipient's system because the message is likely to never reach the recipient's inbox.[238]

While courts have not examined the content of electronic records for factors relating to a message's "spam score," e-mail content has been inspected for factors relating to inconspicuous notice. In *Campbell v. General Dynamics Government Systems Corp.*,[239] an employer initiated a new policy by which all unresolved disputes would be subject to mandatory arbitration.[240] The employees were notified of the new policy via e-mail.[241] Neither the subject heading nor the introductory paragraphs of the e-mail gave any indication that the message was of any importance.[242] While subsequent paragraphs explained that unresolved disputes would now be settled by arbitration, the e-mail did not notify employees that the new policy eliminated the right to resolve disputes in a judicial forum, nor did the e-mail mention that continuation of employment constituted acceptance of the policy's terms.[243] This information was available in the policy itself; however, the policy

235. UETA § 15(a)(2), (b)(2) (1999).
236. *See id.* § 15 cmt. 1.
237. Telephone Interview with Michael Fleming, *supra* note 52; *see supra* Part III.B.
238. *See* UETA § 15(a)(2), (b)(2).
239. 407 F.3d 546 (1st Cir. 2005).
240. *Id.* at 547.
241. *Id.* at 547–48.
242. Campbell v. Gen. Dynamics Gov't Sys. Corp., 321 F. Supp. 2d 142, 144 (D. Mass. 2004), *aff'd*, 407 F.3d 546 (1st Cir. 2005).
243. *Campbell*, 407 F.3d at 548.

was not attached to the e-mail.[244] To access the policy, employees had to follow a hyperlink that led to a page on the company's intranet site.[245] The e-mail did not require a response from employees acknowledging receipt or their understanding of the new policy.[246]

When an employee sought judicial review of his termination over a year later, the company asserted that the employee's dispute should be resolved through arbitration as described by the policy.[247] Although the employee conceded that the e-mail technically was "received,"[248] he argued that the arbitration agreement was not binding because the content of the e-mail belied the importance of the subject matter—the renouncement of an important legal right.[249]

The court relied on the content of the e-mail in determining that the message did not provide fair warning to the employee.[250] The court found that the e-mail "undersold the significance of the Policy" because neither the subject heading nor the text put the recipient on notice "that arbitration was to become mandatory and thereby extinguish an employee's access to a judicial forum as a means for dispute resolution."[251] The court also examined the "tone and choice of phrase[s]" within the e-mail and found them to be lacking.[252] Although the policy itself was written in "clear, contractual language," the e-mail "downplay[ed] the obligations set forth in the Policy."[253] It did not explicitly state that the policy would eliminate an employee's right to seek judicial review and that the policy was legally binding if the recipient continued employment.[254] To paraphrase using the language of UETA, the e-mail was not "in a form capable of being processed" by the *recipient*

244. *Id.*
245. *Id.*
246. *Id.*
247. *Id.* at 549.
248. *Id.* at 548–49 (presenting evidence that e-mail was "opened . . . two minutes after it was sent" but not that it was read).
249. *See id.* at 549 ("[T]he company's e-mail communication had failed to give the plaintiff adequate notice that the Policy was intended to form a binding agreement to arbitrate.").
250. *Id.* at 557.
251. *Id.* at 558.
252. *Id.* at 557.
253. *Id.*
254. *Id.* at 557–58.

because it did not provide him with notice of its importance.[255]

Similarly, an electronic record with spam characteristics is not "in a form capable of being processed" by the *recipient's system* because it resembles spam rather than an important communication.[256] By using language and conventions that raise an electronic record's "spam score," a sender may "trick" the spam filter into believing that a message is unimportant and potentially harmful.[257] As in *Campbell*, the "tone and choice of phrases" used in such a message "downplay" the message's importance because the recipient's filter is likely to misinterpret the message and filter it before it reaches the recipient's inbox.[258] A message with a high spam score may fail to put the spam filter on notice that the message should be delivered to the inbox rather than sent to the junk mail folder (or deleted altogether).[259]

In conclusion, a sender who deliberately or negligently creates a message with a high spam score may fail to send a message "in a form capable of being processed" by the recipient's system; therefore, the message is neither sent nor received.[260] If so, the sender should be responsible for the recipient's lack of awareness of the message because the sender was in the best position to prevent the spam filter from intercepting the message.

2. Factors Controlled by the Recipient

The recipient has no influence over the content and dispatch of an electronic record; thus, the factors under its control are more limited than those of the sender. However, the recipient does control the location of its spam filters and the intensity of those filters.[261] If an overactive spam filter within the recipient's system incorrectly intercepts a legitimate message (i.e., a message without

255. *See* UETA § 15(a), (b) (1999).

256. *See id.* § 15(b).

257. *See Campbell*, 407 F.3d at 557 ("[T]he e-mail announcement . . . downplay[ed] the obligations set forth in the [p]olicy.").

258. *Id.* at 557–58.

259. *See id.* at 557 ("[T]he e-mail communication, in and of itself, was not enough to put a reasonable employee on inquiry notice of an alteration to the contractual aspects of the employment relationship."); *cf.* Whitaker, *supra* note 47, at 24–25 (noting that the Federal Trade Commission requires the content of online notices to be "reasonably understandable and designed to call attention to the information that must be disclosed.").

260. *See* UETA § 15(a), (b).

261. *See* Bowles et al., *supra* note 81, at 13 ("[S]pam filters . . . can be configured in various ways . . . .").

the defects described in Part IV.C.1), the message is likely received because it already entered the system.[262] In such a situation, the recipient has the responsibility to check the junk mail folder or be held responsible for receipt of the message.[263] But what if the filter is located outside of the recipient's system or is maintained by a third party employed by the recipient?

According to the language of UETA, an electronic record is not received until it enters the recipient's "information processing system,"[264] which is defined as "an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information."[265] The UETA comments provide that the "key aspect" of an information processing system is that the user is able to access it.[266] This suggests that an information processing system, viewed broadly, may encompass more than the system itself, so long as the user retains access.[267]

Moreover, the UETA comments assert that the UETA definition of "information processing system" is consistent with the Model Law's definition of "information system."[268] *The Model Law Guide to Enactment* provides: "The definition of 'information system' is intended to cover the *entire range* of technical means used for transmitting, receiving and storing information."[269] Using this broader definition, a recipient would likely be held responsible for spam filters *under its control*, even if outside of the recipient's system, because the filters are within the recipient's "entire range" of access.[270]

Additionally, an analogy to paper mail suggests that a broad definition of the recipient's system likely includes spam filters operated by a third-party agent of the recipient. Courts have universally held that process is received by a corporation when it is acquired by an agent authorized to receive such documents.[271]

262. *See* UETA § 15(b)(1).
263. Telephone Interview with Michael Fleming, *supra* note 52.
264. UETA § 15(b)(1).
265. *Id.* § 2(11).
266. *Id.* § 2 cmt. 9.
267. Telephone Interview with Michael Fleming, *supra* note 52; *see* UETA § 2 cmt. 9.
268. UETA § 2 cmt. 9; *see* Model Law, *supra* note 32, art. 2(f) (providing an almost identical definition).
269. UNCITRAL, *supra* note 21, at 29 (emphasis added).
270. Telephone Interview with Michael Fleming, *supra* note 52; *see* UNCITRAL, *supra* note 21, at 29.
271. Tech Hills II Assocs. v. Phx. Home Life Mut. Ins. Co., 5 F.3d 963, 968

Since the agent has specifically been chosen by the corporation to receive process, courts reason that receipt occurs when the agent receives the process rather than when the process actually comes into the hands of the corporation.[272] Courts fear that establishing receipt as the time the corporation receives the process would result in "lost homework" excuses where the corporation asserts it did not receive the process until long after it had been received by the agent.[273]

Although there is no "bright-line rule" regarding who is authorized to receive process, courts have found service of process to be sufficient when received by agents and employees who are "responsible and sufficiently familiar with legal matters" and who can "forward the pleading to the proper individual or department within the company."[274] Thus, service to a "run-of-the-mill corporate employee"[275] or to a security guard[276] would not result in receipt, while service to a company's receptionist, local store manager, or CEO would result in receipt.[277] Similarly, a notice is received under the Revised U.C.C. when "it is duly delivered . . . at the place of business through which the contract was made *or at another location held out by that person as the place for receipt of such communications.*"[278]

A third-party spam filter should be regarded as a "receptionist" rather than a "security guard." The filter has been "chosen" by the recipient (or the recipient's system manager) and is "authorized to

(6th Cir. 1993); Barr v. Zurich Ins. Co., 985 F. Supp. 701, 702 (S.D. Tex. 1997); *see* Reece v. Wal-Mart Stores, Inc., 98 F.3d 839, 843–44 (5th Cir. 1996) ("[Sending the pleading to the corporation's CEO] is a perfectly sensible way to notify a responsible individual within the corporation . . . ."); Roe v. O'Donohue, 38 F.3d 298, 304 (7th Cir. 1994); Edling v. IMI Sys., Inc., No. CIV.A. 301CV2817-M, 2002 WL 240135, at *2 (N.D. Tex. Feb. 15, 2002). Although *Murphy Brothers, Inc. v. Michetti Pipe Stringing, Inc.*, 526 U.S. 344 (1999), repealed the so-called "receipt rule" and disallowed informal service of process via fax or photocopy, *Murphy Brothers* does not suggest that *formal service* upon an authorized agent is invalid. *Edling*, 2002 WL 240135, at *2.

272. *See Barr*, 985 F. Supp. at 703 ("Registered agents exist to receive process . . . . Defendant chose this one.").

273. *Edling*, 2002 WL 240135, at *2.

274. *Reece*, 98 F.3d at 843.

275. *Barr*, 985 F. Supp. at 703.

276. *Tech Hills II*, 5 F.3d at 968.

277. *Reece*, 98 F.3d at 843–44 (CEO); Roe v. O'Donohue, 38 F.3d 298, 304 (7th Cir. 1994) (receptionist); Allison v. Montgomery Ward & Co., 159 F. Supp. 550, 551–52 (D.N.H. 1957) (store manager).

278. U.C.C. § 1-202(e) (2001) (emphasis added).

accept" and inspect all of the recipient's messages.[279] Like an agent authorized to receive process, a third-party filter has the capability—and responsibility—to forward the message to the appropriate individual.[280] Moreover, the recipient certainly has identified the third-party spam filter as a "place for receipt" of electronic records because all records must pass through the filter before entering the recipient's system.[281]

If messages could be reviewed by a third-party filter prior to receipt, a recipient could engage in a "lost homework" excuse and potentially avoid receipt by preventing the message from entering her system.[282] Review prior to receipt is contrary to the plan language of UETA because awareness of a message is not a precursor to receipt.[283] Further, allowing such review would result in a media-specific rule (which UETA has expressly avoided) because it would allow agents to receive traditional mail but not electronic mail.[284]

Therefore, barring any sharp or negligent practices on the part of the sender, recipients should be responsible for the actions of their spam filters, even if the filter is located outside of the recipient's system or operated by a third-party agent of the recipient. If a message is incorrectly filtered by an overactive spam filter within the recipient's control, the recipient has a responsibility to check her junk mail folder or otherwise be held responsible for receipt of the message.

3. Application to Hypotheticals

Application of the accountability test to the hypotheticals in Part I demonstrates that the test is a reasonable and balanced approach.[285] In "Awaiting Acceptance," an e-mail was intercepted

279. *See Tech Hills II*, 5 F.3d at 968; *Barr*, 985 F. Supp. at 702–03.

280. *See Reece*, 98 F.3d at 843–44 ("[T]his method of delivery is a perfectly sensible way to notify a responsible individual . . . .").

281. *See* U.C.C. § 1-202(e).

282. *See* Edling v. IMI Sys., Inc., No. CIV.A. 301CV2817-M, 2002 WL 240135, at *2 (N.D. Tex. Feb. 15, 2002); *cf.* Snijders, *supra* note 50, at 80 (arguing in favor of a receipt rule that does not require the recipient to view the message).

283. *See* UETA § 15(e) (1999).

284. *See* UETA Refs. & Annots. Prefatory Note B (West, Westlaw through 2011 annual meetings) (noting that the Act merely seeks to remove "biases and barriers" so that existing law will apply to an electronic context).

285. Additionally, unlike the E-SIGN consumer protection provision, the accountability test can apply to any transaction governed by UETA. *Compare* 15 U.S.C. § 7001(c) (2006) (applying only where a writing is legally required), *with*

due to an overactive spam filter operated by the recipient's agent.[286] Although the filter was located outside of the recipient's system, it was still under the recipient's control; therefore, the e-mail was received.[287] In "Rotten Recall," the sender deliberately doctored an e-mail to ensure that it would be intercepted by a spam filter.[288] The e-mail was not "in a form capable of being processed" by the recipient's system.[289] Since the sender had control over the e-mail's content, the e-mail was not received, even though the message may technically have entered the recipient's system.[290] In contrast, the sender in "Flower Fanatic" did not increase the e-mail's "spam score."[291] Since the recipient had control over, and in fact created, the rule that rerouted the e-mail to a separate folder, the e-mail was received.[292]

Moreover, the accountability test conforms to the underlying policies of UETA.[293] Requiring parties to take responsibility for the factors under their control will result in more certainty as to how UETA is applied.[294] The accountability test is a "reasonable practice" because it encourages each party to take responsibility for its practices and protects parties from sharp or negligent practices.[295] Finally, protecting recipients from unscrupulous senders will "promote public confidence in the validity, integrity and reliability of electronic commerce."[296]

V. CONCLUSION

None of the electronic communication laws discussed in this note command a party to do business electronically.[297] If a party voluntarily elects to benefit from e-commerce, she should be responsible for having some understanding of the required

UETA § 5(b) (applying where parties have "agreed to conduct transactions by electronic means").

286. *See supra* text accompanying note 1.
287. *See supra* Part IV.C.2.
288. *See supra* text accompanying note 2.
289. *See* UETA § 15(a)–(b).
290. *See supra* Part IV.C.1.b.
291. *See supra* text accompanying note 3.
292. *See supra* Part IV.C.2.
293. *See* UETA § 6.
294. *See id.* § 6 cmt. 1(b).
295. *See id.* § 6(2).
296. *Id.* § 6 cmt. 1(f).
297. *See* 15 U.S.C. § 7001(b)(2) (2006); Convention, *supra* note 32, art. 8, para. 2; UCITA § 107(b) (2002); UETA § 5(a).

technology. In the paper world, a sender could not argue that a letter with the incorrect address was properly sent.[298] A recipient could not argue that a letter was not received because she did not know where the mailroom was.

In the electronic world, it should be the same. While senders and recipients should be protected from unfair practices, they must have a general understanding of the system in which they conduct business. This includes taking responsibility of the dispatch and receipt factors under each party's control. While understanding complex electronic communication processes may involve a sharp learning curve, that is simply "the cost of doing e-business."

298. *See, e.g.*, Int'l Television Film Prod., Inc. v. Comm'r, 45 T.C.M. (CCH) 1049 (1983).