



1-1-2017

Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software?

Stacy-Ann Elvy
New York Law School

Follow this and additional works at: <https://scholarlycommons.law.wlu.edu/wlulr>



Part of the [Science and Technology Law Commons](#)

Recommended Citation

Stacy-Ann Elvy, *Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software?*, 74 Wash. & Lee L. Rev. 77 (2017).

Available at: <https://scholarlycommons.law.wlu.edu/wlulr/vol74/iss1/4>

This Article is brought to you for free and open access by the Washington and Lee Law Review at Washington and Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Law Review by an authorized editor of Washington and Lee University School of Law Scholarly Commons. For more information, please contact christensena@wlu.edu.

Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software?

Stacy-Ann Elvy*

ABSTRACT

The Internet of Things (IOT) has been described by the American Bar Association as “one of the fastest emerging,” potentially most “transformative and disruptive technological developments” in recent years. The security risks posed by the IOT are immense and Article 2 of the UCC should play a central role in determinations regarding liability for vulnerable IOT products. However, the lack of explicit clarity in the UCC on how to evaluate Article 2’s applicability to hybrid transactions that involve the provision of goods, services, and software has led to conflicting case law on this issue, which contradicts the UCC’s stated goals of uniformity and simplicity. The Article contends that the existing approaches used to evaluate whether Article 2 applies to a hybrid transaction are inadequate for assessing IOT contracts and that IOT technology will increase the complexity and frequency of existing hybrid transactions. Ultimately, the Article proposes and evaluates four solutions for determining whether Article 2 should apply to IOT transactions to provide uniformity, simplicity, and clarity in this area. The Article argues that a functionality approach is preferable as it effectively considers the unique manner in which services and software are provided in connection with the sale of IOT devices. Under the functionality test, hybrid transactions involving goods, software, and services are subject to Article 2 where the services and

* Associate Professor of Law, New York Law School (J.D., Harvard Law School; B.S., Cornell University). I am grateful to my colleagues at New York Law School for their valuable comments and insights. I would also like to thank my research assistants Victoria Stork and Niyati Sangani. Finally, I would like to thank my In-Charge-Editor, Kiersty DeGroote, and the rest of the W&L Law Review for their hard work on this Article.

software advertised by the manufacturer and retailer are integral to the device's operations.

Table of Contents

I. Introduction	78
II. The Complexity of Hybrid IOT Transactions	91
A. Mechanics of Hybrid IOT Transactions	91
B. Distinctions Between IOT and Other Hybrid Transactions.....	97
III. The Inadequacy of Current Approaches in the IOT Era.....	104
A. Services and Goods under Article 2	104
1. Predominant Purpose Test.....	105
2. Gravamen of the Claim Test	112
B. Service Contracts and Other Sources of Law.....	114
1. Common-Law Warranties	114
2. Federal Warranty Act	119
C. Software and Goods Under Article 2	125
D. Software and Other Sources of Law	136
IV. Proposals	142
A. Products Approach	144
B. Functionality Approach.....	148
C. Article 9's Embedded Approach.....	165
D. Exclusionary Approach	169
V. Conclusion	170

I. Introduction

The uniformity of state laws has numerous benefits including promoting predictability and stability, and the elimination of extant legal principles in favor of more efficient and adaptable rules.¹ With the goals of uniformity and

1. See Paul B. Stephan, *The Futility of Unification and Harmonization in International Commercial Law*, 39 VA. J. INT'L L. 743, 746–52 (1999) (“A legal

modernization in mind, Karl Llewellyn and others began drafting the Uniform Commercial Code (UCC).² Today, the UCC is the primary source of commercial law in the United States. The code was created to reduce contrasting state approaches to commercial law.³ Thus, the UCC was intended to make uniform, simplify, clarify and modernize state laws on commercial transactions.⁴

Article 2 of the UCC (Article 2) governs transactions in goods.⁵ However, despite the goals of certainty and uniformity, one of the thorniest issues in sale of goods transactions is how best to determine whether Article 2 applies to transactions involving the provision of goods and non-goods, such as services or software.⁶ Courts have historically struggled to determine whether Article 2 applies to these types of hybrid transactions

system that allows people to form clear legal commitments with predictable consequences makes it easier for people to rely on each other”); *see also* Benjamin Geva, *Uniformity in Commercial Law: Is the UCC Exportable*, 29 *LOY. L.A. L. REV.* 1035, 1038 (1996) (describing predictability and modernization of laws as a byproduct of uniformity).

2. *See* Karl N. Llewellyn, *The First Struggle to Unhorse Sales*, 52 *HARV. L. REV.* 873, 876 (1939) (“[Judgements] in 1870 to 1900 . . . [are] *noncharacteristic* . . . [and] do not afford guidance measurably transcending the accident of judicial personnel.”); Geva, *supra* note 1, at 1039 (describing modernization and uniformity as the goals of the drafters of the UCC).

3. *See* E. Hunter Taylor, Jr., *Recent Developments in Commercial Law: Federalism or Uniformity of Commercial Law*, 11 *RUTGERS L.J.* 527, 530 (1980) (describing the failure of previous uniform laws on commercial law, such as the Uniform Sales Act, to achieve uniformity); Arthur L. Corbin, *The Uniform Commercial Code—Sales; Should It Be Enacted?*, 59 *YALE L.J.* 821, 834–35 (1950) (“But after the 50 years through which we have just lived, the old rules need some replacement, the old words need changing, the analysis and organization can be improved, the remedies can be made more effective.”); U.C.C. § 1-103 (AM. LAW INST. & UNIF. LAW COMM’N 2001) (stating that the Uniform Commercial Code should be construed liberally to promote its underlying purposes).

4. U.C.C. § 1-103 (AM. LAW INST. & UNIF. LAW COMM’N 2001).

5. *Id.* § 2-102.

6. *See* Richard Raysman & Peter Brown, *Applicability of the UCC to Software Transactions; Technology Today*, N.Y. L.J. ONLINE (Mar. 8, 2011), <http://www.newyorklawjournal.com/id=1202484668508/Applicability-of-the-UCC-to-Software-Transactions> (last visited Mar. 5, 2017) (acknowledging that Article 2 does not explicitly mention software) (on file with the Washington & Lee Law Review).

and they continue to do so today.⁷ Various approaches, such as the predominant purpose test, have been offered by commentators to address this lack of explicit clarity in Article 2.⁸

Even within jurisdictions that have adopted the predominant purpose test, courts often use different factors to assess whether the predominant purpose of the transaction is for the provision of goods or services.⁹ As a result, there is a lack of consensus on what transactions are subject to Article 2.¹⁰ A number of courts have applied Article 2 to transactions involving software, while other courts have reached the opposite conclusion.¹¹ In a 2016 district court case involving Article 2's role in a software transaction the court stated:

7. *See id.* (noting that courts continue to struggle with hybrid software transactions that include custom development and the provision of services).

8. *See* J.O. Hooker & Sons, Inc. v. Roberts Cabinet Co., 683 So. 2d 396, 400 (Miss. 1996) (discussing courts that have reached different conclusions over whether the UCC should apply to a mixed transaction of goods and services); Anthony Pools v. Sheehan, 455 A.2d 434, 441 (Md. 1983) (“[T]he provisions of the Maryland U.C.C. dealing with implied warranties apply to consumer goods, even if the transaction is predominantly one for the rendering of consumer services.”); *see also* 1 WILLIAM D. HAWKLAND, UNIFORM COMMERCIAL CODE SERIES § 2-102:4 (2008) (“This stated limitation on the scope of Article 2 is not as absolute as it seems. In some circumstances, both Article 2 and Article 9 will apply to the transaction.”).

9. *See infra* Part III.A and accompanying notes 35–51 (discussing the rapid expansion of IOT devices and the consequent security risks presented).

10. Scholars have also decried Article 2's lack of uniformity on other important issues, such as the extension of warranties to third party beneficiaries. *See* E. Hunter Taylor, Jr., *Uniformity of Commercial Law and State-by-State Enactment: A Confluence of Contradictions*, 30 HASTINGS L.J. 337, 343 (1978) (illustrating the lack of uniformity from the issue of warranty and privity); *see also* Jennifer Camero, *Two Too Many: Third Party Beneficiaries of Warranties Under the Uniform Commercial Code*, 86 ST. JOHN'S L. REV. 1, 12–21 (2012) (“[S]ection 2-318 produces a lack of uniformity among the states that defeats the UCC's purpose, generates unpredictable seller liability, and creates unnecessary disputes over applicable law.”).

11. *See* Olcott Int'l & Co. v. Micro Data Base Sys., Inc., 793 N.E. 2d 1063, 1071 (Ind. Ct. App. 2003) (applying Article 2 to contracts to purchase pre-existing software modules); *see also* Advent Sys. Ltd. v. Unisys Corp., 925 F.2d 670, 676 (3d Cir. 1991) (identifying the benefits of applying the UCC to computer software transactions); Recursion Software, Inc. v. Interactive Intelligence, Inc., 425 F. Supp. 2d 756, 786 (N.D. Tex. 2006) (assuming the Texas UCC applies to software licenses); Sagent Tech. Inc. v. Micro Sys., Inc., 276 F. Supp. 2d 464, 466 (D. Md.

The applicability of the Uniform Commercial Code to software is a question that has confounded courts in the digital age. For every court that finds that the weight of authority favors application of common law and not the UCC with regard to software licenses, another finds that courts nationally have consistently classified the sale of a software package as the sale of a good for UCC purposes.¹²

Other complications arise in software transactions where software is combined with hardware or where other products are provided with the software.¹³ Such agreements may be viewed as hybrid transactions and evaluated under the predominant purpose test.¹⁴ Assuming that the software is viewed as a good rather than a service, a hybrid transaction may also arise where additional services, such as support services, are provided in connection with the software. Even in cases in which software is

2003) (finding the UCC applies to the sale of computer software otherwise labeled as licenses); *Pearl Inv., LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326, 352 (D. Me. 2003) (“[T]he test for inclusion or exclusion from Article 2 [of the UCC] is not whether the goods and non-goods parts of the contract are mixed, but rather, whether their predominant factor . . . is a transaction of sale.”); *I. Lan Sys., Inc. v. Netscout Serv. Level Corp.*, 183 F. Supp. 2d 328, 332 (D. Mass. 2002) (“[T]he UCC technically does not govern software licenses . . . but with respect to the 1999 transaction, the UCC best fulfills the parties’ reasonable expectations.”); *Wachter Mgmt. Co. v. Dexter & Chaney, Inc.*, 144 P.3d 747, 751 (Kan. 2006) (finding that computer software is a good under Article 2 even where incidental services are provided); *Data Processing Servs., Inc. v. L.H. Smith Oil Corp.*, 492 N.E.2d 314, 318 (Ind. Ct. App. 1986) (declining to apply Article 2 where a computer programming business only developed a processing system and did not sell hardware).

12. *SAS Inst., Inc. v. World Programming Ltd.*, No. 5:10-25-FL, 2016 WL 3435196, at *10 (E.D.N.C. June 17, 2016).

13. *See Arlington Electrical Constr. v. Schindler Elevator Corp.*, 1992 WL 43112, at *4–7 (stating that the sale of software and hardware in a single agreement is a sale of goods and not services, but noting that the predominant purpose test applies to determine whether the transaction is subject to Article 2); *see also Waterfront Props., Inc. v. Xerox Connect, Inc.*, 58 U.C.C. Rep. Serv. 2d (West) 809 (W.D.N.C. Jan 31, 2006) (applying Article 2 to a transaction involving hardware and software); Keith A. Rowley et al., *Uniform Commercial Code Survey: Sales*, 62 BUS. LAW. 1559, 1559–61 (2007) (discussing the Waterfront case and other mixed transactions and contending that courts narrowly interpret the scope of Article 2).

14. *See Schroder’s, Inc. v. Hogan Sys., Inc.*, 741–42, 522 N.Y.S. 2d 404, 406 (1987) (describing the combination of hardware and software as a hybrid agreement).

provided without hardware, but is accompanied by development or implementation services, courts are still faced with the question of whether the transaction is governed by Article 2.¹⁵

The lack of clarity in this area affects both consumer and non-consumer transactions.¹⁶ Rather than achieving uniformity and simplicity, the UCC has “produced variety and [likely] greater contracting risk” in certain areas.¹⁷ The uncertainty on this subject is glaring as the UCC, in contrast, provides specific guidance on how to distinguish between a lease and a sale of goods with a reserved security interest.¹⁸

The impact of this ambiguity in Article 2 becomes more pressing in the age of the Internet of Things (IOT).¹⁹ Companies

15. See *Wharton Mgmt. Grp. v. Sigma Consultants*, 1990 WL 18360, at *7–8 (Del. Super. Ct. Jan. 29, 1990) (finding that the services aspect of a transaction for the design, development and installation of software, without the sale of hardware, dominated the subject matter of the transaction, thereby removing the transaction from the scope of Article 2).

16. See *Howard Dodge & Sons, Inc. v. Finn*, 391 N.E. 2d 638, 640 (Ind. Ct. App. 1979) (describing the sale of air conditioning and heating equipment with installation); see also *Aluminum Co. of Am. v. Electro Flo Corp.*, 451 F.2d 1115, 1116 (10th Cir. 1971) (regarding the design and supply of aluminum floor material); *Holstad v. Southwestern Porcelain, Inc.* 421 N.W.2d 371, 372 (Minn. Ct. App. 1988) (discussing the purchase and installation of stock farm silo).

17. See Robert E. Scott, *Rethinking the Uniformity Norm in Commercial Law: Optimal Institutional Design for Regulating Incomplete Contracts*, in *THE JURISPRUDENCE OF CORPORATE AND COMMERCIAL LAW* 149, 193 n.2 (Jody S. Kraus & Steven D. Walt eds., 2000) (“[R]ecent scholarship criticizes the incorporation strategy for interpretation as well.”).

18. See U.C.C. § 1-203(a)–(e) (AM. LAW INST. & UNIF. LAW COMM’N 2001) (“Whether a transaction in the form of a lease creates a lease or security interest is determined by the facts of each case” and providing guidance on making such determinations). There have been previous failed attempts to amend Article 2 to clarify Article 2’s definition of goods. For instance, the 2003 withdrawn amendments to Article 2 explicitly excluded information from the definition of goods. See *id.* § 2-103(k) (specifying what the term “goods” includes and excludes).

19. The IOT is a network of connected devices which collect, store, communicate, and transmit information to each other and associated systems. See Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 840 (2016) (contending that the IOT will worsen preexisting information asymmetry in consumer contracts to the benefit of companies, increase the lack of proximity between consumers and the contract formation process, discourage understanding of contract terms, and that common law agency principles, e-commerce statutes, and contract law are unlikely to effectively address such concerns).

are increasingly adopting a software and service centric approach to the development and sale of goods.²⁰ Today, consumers frequently purchase and easily integrate Internet-enabled devices into their daily lives and activities.²¹ IOT devices can purchase goods without human intervention and monitor consumption rates.²² These products can also collect and report to manufacturers and retailers status and location data, as well as information about device users and individuals in their households.²³ With the development of the IOT, companies routinely offer services, goods, and software to buyers in a single transaction.²⁴ For example, in connection with the sale of an Indoor Nest Cam, Nest provides software updates and offers a subscription service that sends motion alerts to smartphones, saves past videos, in Nest's cloud-based server, and allows owners to rewind, share, and create time-lapses.²⁵ Almost any product including cars, everyday household and office goods, and manufacturing equipment can be accompanied by cloud or fog computing services, firmware, software updates, and ongoing online services that facilitate interconnectivity between individuals, companies, and systems.²⁶

20. *See id.* at 840 (“Today, merchants frequently use electronic shopping agents in automated transactions to buy and sell goods.”).

21. *See id.* (explaining how IOT maximizes individual efficiency by consolidating products, systems, and platforms into a single network).

22. *See id.* (“IOT robotic devices are revolutionizing the way that consumers shop . . . Consumers no longer need to log on to a company’s website or use a mobile application to purchase goods.”).

23. *See id.* at 841 (“Digital tracking technology embedded within IOT devices and smart labels could permit a manufacturer or retailer to advertise additional products to consumers once a product is in the consumer’s home or office based on the data generated by the device.”).

24. *See id.* (“[D]ata generated by IOT devices could be used to target vulnerable consumers for contracting.”).

25. *See What You Get with a Nest Aware Subscription for Your Camera*, NEST SUPPORT, <https://nest.com/support/article/What-do-I-get-with-Nest-Aware-for-Nest-Cam> (last updated Sep. 9, 2016) (last visited Mar. 5, 2017) (providing a comparison chart of the beneficial features attached to a Nest Aware subscription) (on file with the Washington and Lee Law Review). Every Nest Cam and Dropcam comes with a free trial of Nest Aware, the subscription service, with video history. *See id.* (allowing for a free trial lasting thirty days).

26. *See Elvy, supra* note 19, at 841 (“Goods can be made with a readable element in the packaging, which will allow manufacturers to assess, in real time

Consider that in 2016 the manufacturer of Revolv, a smart home hub that allowed owners to control multiple devices in their homes through a smartphone application, announced that services would no longer be provided to support the device.²⁷ This rendered the device all but useless to buyers who purchased the product, which retailed at \$299.²⁸ Owners of the Revolv device have not only spent funds to acquire the device but also have incorporated the device into their daily lives and activities, including allowing the device to potentially collect data about their in-home activities. Now, suppose that the Revolv hub device or a similar IOT device is vulnerable to hackers who could access data collected by the device,²⁹ or remotely control the

the types of consumers who are buying and using their product.”).

27. See Alissa Walker, *If You Use Revolv’s Smart Hub, You Are Officially Screwed (Thanks Nest!)*, GIZMODO (Apr. 4, 2016, 5:45 PM), <http://gizmodo.com/nest-owned-smart-hub-gets-permanently-killed-1768977505> (last visited Mar. 5, 2017) (shutting down all support for the Revolv hub and its smartphone apps to introduce an improved version) (on file with the Washington and Lee Law Review); see also Stephen Lawson, *Why Nest’s Revolv Hubs Won’t be the Last IOT Devices Knocked Offline*, CIO (Apr. 4, 2016, 4:05 PM), <http://www.cio.com/article/3051188/internet-of-things/why-nests-revolv-hubs-wont-be-the-last-iot-devices-knocked-offline.html> (last visited Mar. 5, 2017) (“Devices that rely on cloud-based software are inherently vulnerable to getting left behind if that software gets shut down, but IoT raises the stakes.”) (on file with the Washington and Lee Law Review).

28. See Althea Chang, *Nest to Disable Revolv Hub, Mulls Paying Back Users*, CNBC (Apr. 6, 2016, 2:04 PM), <http://www.cnbc.com/2016/04/06/nest-to-disable-revolv-hub-mulls-paying-back-users.html> (last visited Mar. 5, 2017) (working to compensate customers who have been using the Revolv smart home system) (on file with the Washington and Lee Law Review). While it has been suggested that buyers may receive some compensation for the service cancellation, it is not entirely clear whether any such compensation will adequately compensate purchasers. See *id.* (“The company would not disclose exactly how Revolv users would be compensated or whether their Revolv devices could be replaced by Nest devices.”).

29. See Kat Greene, *J&J Says Insulin Device Can Be Hacked But Risk is Low*, LAW360 (Oct. 4, 2016, 10:10 PM), <http://www.law360.com/articles/848402/j-j-says-insulin-device-can-be-hacked-but-risk-is-low> (last visited Mar. 5, 2017) (recommending that users of OneTouch Ping insulin pump should take precautions) (on file with the Washington and Lee Law Review); see also Melissa Daniels, *St. Jude Heart Devices Have Security Weaknesses, Suit Says*, LAW360 (Aug. 29, 2016, 5:26 PM), <http://www.law360.com/articles/833622/st-jude-heart-devices-have-security-weaknesses-suit-says> (last visited Mar. 5, 2017) (describing security flaws in IOT pacemakers and the potential for hackers to tamper with the device’s functions or the information collected by the device) (on file with the

device. Should owners of such devices have a cause of action under Article 2 where a manufacturer elects to terminate the services and software updates that are integral to the device's operations or where a manufacturer's database or a device is hacked and a consumer's data is leaked or the device malfunctions as a result? This Article seeks to answer these questions.

If a court were to determine that Article 2 does not apply to a Revolv hub transaction, the common law would likely be applicable to the dispute. Contracts that are subject to Article 2 typically obtain the benefit of various implied warranties including the implied warranty of merchantability, unless such warranties have been effectively disclaimed.³⁰ These warranties can be particularly beneficial to buyers who were not provided with an express warranty. IOT manufacturers may exclude the services and software that they provide from the express warranties that cover a device's hardware.³¹ The failure of an IOT manufacturer to secure an IOT device or the data generated by an owner's use of an IOT device should serve as the basis for breach of implied warranty claims under Article 2.³² However, such claims in the data breach scenario are more likely to be viable where the transaction is subject to Article 2.³³

Washington and Lee Law Review).

30. See U.C.C. § 2-314(1) (AM. LAW INST. & UNIF. LAW COMM'N 2012) (“[A] warranty that the goods shall be merchantable is implied in a contract for their sale if the seller is a merchant with respect to goods of that kind.”); *id.* § 2-314(3) (“[O]ther implied warranties may arise from course of dealing or usage of trade.”).

31. See generally discussion *infra* Part III and accompanying notes.

32. See *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 954–59 (S.D. Cal. 2014) (detailing how plaintiffs alleged that defendant breached the implied Article 2 warranties and that by creating, marketing, and selling PS3s and PSPs, the defendant represented and warranted that its online services and networks were merchantable, fit for their intended purposes, and provided adequate security for the plaintiffs' personal information); *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 119 (2009) (detailing how the plaintiff asserted that the defendant breached the implied warranty of fitness for a particular purpose by failing to secure consumer data and its electronic payment system, which was used by the plaintiffs to purchase groceries from the defendant).

33. See generally discussion *infra* Part III and accompanying notes.

To avoid the application of Article 2, IOT companies may separate the services and software from the sale of the device by providing different agreements that govern the device's hardware, software and services.³⁴ A defendant may respond to a suit involving a breach of warranty claim by arguing that Article 2 does not apply to the transaction or that all warranties have been effectively disclaimed.³⁵ In fact, a company facing a data breach lawsuit may successfully defend against Article 2 breach of implied warranty claims by contending that the services provided in connection with the device do not qualify as a good under Article 2 and therefore the implied warranties are not applicable.³⁶

There will be thirty-four billion IOT devices by 2020 and nearly six trillion dollars will be spent on IOT solutions over the

34. See Sarah Howard Jenkins, *Contracting Out of Article 2: Minimizing the Obligation of Performance & Liability for Breach*, 40 LOY. L.A. L. REV. 401, 410–11 (2007) (discussing the “predominant feature” test courts use to determine whether to apply Article 2). End User Licensing Agreements may also be used in hybrid software transactions to prevent application of the first sale doctrine under copyright law. See 17 U.S.C. § 109(a) (2006) (“[T]he owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord.”); see also Lothar Determann & Aaron Xavier Fellmeth, *Don't Judge a Sale by Its License: Software Transfers Under the First Sale Doctrine in the United States and the European Community*, 36 U.S.F. L. REV. 1, 29, 35 (2002) (noting that courts disregard how parties label the transaction by assuming there is a sale of goods when a software copy is transferred perpetually against a lump sum payment). Companies may also use End User Licensing Agreements to facilitate price discrimination, which allows licensors to charge customers based on the prices that they are willing to pay. As a result, large companies frequently pay more than smaller ones or individuals, especially where pricing is based on the number of users or type of use. See Jean Braucher, *When Your Refrigerator Orders Groceries Online and Your Car Dials 911 After an Accident: Do We Really Need New Law for the World of Smart Goods?*, 8 WASH. U. J.L. & POL'Y 241, 253–54 (2002) (noting that price discrimination is legal when it is not accompanied by efforts to undermine competitors).

35. See *Anthony Pools v. Sheehan*, 455 A.2d 434, 436 (Md. 1983) (“Anthony contends that the Sheehan’s swimming pool is not ‘goods,’ that exclusion of implied warranties is allowed, and that a directed verdict on the plaintiffs’ warranty count was proper.”).

36. See *Sony Gaming Networks*, 996 F. Supp. 2d at 980 (“Sony moves to dismiss . . . the statutory claims fail because network services are not ‘goods’ as defined under the Uniform Commercial Code (UCC).”).

next five years.³⁷ As the American Bar Association has noted, the rapid expansion of the IOT will require legal scholars, companies, consumer protection advocates, regulators, legislators, and lawyers to “identify and address potential risks and liabilities.”³⁸ The security risks posed by IOT products are immense as evidenced by a recent distributed denial of service attack conducted by hackers who weaponized vulnerable IOT devices to interrupt access to major websites.³⁹ These security concerns may be due in part to the failure of IOT companies to invest in building effective security measures into their devices. The application of Article 2, along with its implied warranties to transactions involving IOT products, may encourage IOT companies to effectively address these security concerns.

Elsewhere, I have argued that the new, automatic, and interface-free contracting environment generated by the IOT creates difficulties in assessing consumer assent to contract terms in a manner that compels a revision of applicable legal rules.⁴⁰ My previous scholarship in this area acknowledged that Article 2 may apply to certain IOT transactions.⁴¹ However, given the current lack of uniformity in dealing with hybrid contracts,⁴² it is unclear whether all IOT transactions will be

37. See John Greenough & Jonathan Camhi, *Here Are IoT Trends That Will Change the Way Businesses, Governments, and Consumers Interact with the World*, BUS. INSIDER (Aug. 29, 2016, 10:18 AM), <http://www.businessinsider.com/top-internet-of-things-trends-2016-1> (last visited Mar. 5, 2017) (forecasting the emerging IoT market through megatrends, device growth, and potential returns on investment) (on file with the Washington and Lee Law Review).

38. *Internet of Things*, INTERNET OF THINGS (IoT) NAT'L INST. (2016), http://www.americanbar.org/content/dam/aba/events/science_technology/2016/iot_brochure.authcheckdam.pdf.

39. Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. TIMES (Oct. 21, 2016), http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0 (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

40. See Elvy, *supra* note 19, at 839 (“This Article suggests important amendment to Article 2 and argues that courts should adjust their application of existing contract law and agency principles to account for the new automatic and interface-free contracting environment that the age of the IOT will herald.”).

41. See *id.* at 859 (discussing the ability of the IOT device to consent to agency, thus imposing contractual liability on the principal).

42. See Raysman & Brown, *supra* note 6 (“As evidence by several decisions

subject to Article 2. This has important implications for the legal framework which will govern disputes involving IOT products. This Article builds on my previous work on the IOT by evaluating the question of whether (and under what circumstances) hybrid IOT transactions should be governed by Article 2.⁴³

Ultimately, this Article contends that the existing approaches currently employed to assess Article 2's applicability to hybrid contracts are wholly inadequate for IOT transactions. Further, the widespread effective application of other legal frameworks, such as the American Law Institute's (ALI) Principles on the Law of Software Contracts (Software Principles)⁴⁴ to hybrid IOT transactions is questionable. IOT technology will increase the complexity and frequency of existing hybrid transactions, with ongoing relationships being created between the buyer, the retailer and the manufacturer. As will be shown below, this level of intricacy cannot be effectively resolved under current approaches designed to deal with hybrid transactions.

Consider a business that would like to sue a seller for breach of warranties under Article 2 because of defective IOT manufacturing equipment and services that negatively impacted its production schedule and output. Assume further that the IOT manufacturing device, which was built and installed by the seller, contained embedded software and the seller contracted to provide cloud-computing services and

in the past year, courts continue to wrestle with mixed software licensing transactions that include custom development and the provision of services.”).

43. While scholars, such as Jean Braucher, have addressed hybrid transactions involving software and goods in the non-IOT context, this Article analyzes hybrid IOT transactions that involve not only the sale of goods and software but also the provision of ongoing services, such as mobile applications, and associated software updates and cloud computing, all of which are needed to permit the devices to achieve full functionality. See Jean Braucher, *Contracting Out of Article 2 Using a “License” Label: A Strategy That Should Not Work for Software Products*, 40 LOY. L.A. L. REV. 261, 262 (2006) (contending that software product transactions, even if labeled “licenses” should be treated as sales for purposes of applying Article 2).

44. AM. LAW INST., PRINCIPLES OF THE LAW OF SOFTWARE CONTRACTS §§ 1.06(a), 2.02 (2010) [hereinafter Software Principles].

software updates. Whether Article 2 would automatically apply to such a contract is unsettled under current law. The lack of clarity on the issue of whether Article 2 applies to hybrid transactions belies the UCC's stated goals of uniformity and simplicity and can lead to unwarranted disputes between parties about the laws applicable to a transaction. Parties entering into such transactions are unable to definitively determine whether Article 2 will apply to their hybrid transaction before contracting.⁴⁵ While some vagueness in the language of any uniform code can be expected, the provisions related to the code's scope should not be ambiguous.

In keeping with the stated goals of the UCC, this Article offers four solutions to promote uniformity and clarity in this area, but ultimately advocates for the adoption of a functionality approach. Under each proposal, all parties involved in a hybrid IOT transaction would know prior to contracting whether Article 2 applies to the transaction. Further, courts would no longer need to engage in the time consuming process of attempting to apply vague tests or multiple and different factors to determine Article 2's applicability to such transactions. This would also eliminate the conflicting holdings often found in case law addressing hybrid transactions.

First, under a products approach, the scope of Article 2 would be expanded to explicitly cover transactions involving "products," which would include the sale of IOT devices, the software built into these devices, software updates and all device services offered by manufacturers or retailers, including product ordering and monitoring services. Second, under a functionality test, Article 2 would apply to a hybrid IOT transaction where IOT devices are sold with ongoing services and software that are necessary to enable the device to function as advertised. Thus, if the IOT device cannot fully operate without the accompanying

45. While most consumers are likely unaware of the UCC, legal counsel for companies entering into IOT transactions may be particularly concerned about the law that governs an agreement prior to contracting, as the applicable source of law can impact a client's rights and obligations under a contract. See Raysman & Brown, *supra* note 6 ("[T]he application of the UCC to a software transaction can be an important consideration that can radically change the remedies or viability of the parties' claims in a dispute.").

service and software provided by the manufacturer or retailer, the transaction should be subject to Article 2. In the consumer setting, buyers could be protected by non-disclaimable implied warranties that apply to the device, and the ongoing services and software that are needed for the device to function.⁴⁶ Third, under an exclusionary approach, Article 2 would be revised to exclude hybrid IOT transactions. Fourth, to resolve the ambiguity in this area, Article 2 could be amended to adopt Article 9's embedded approach to the definition of goods.⁴⁷ The Article concludes by suggesting that the adoption of a functionality approach is preferable. The functionality test accounts for the remarkable manner in which services and software are provided in connection with the sale of IOT devices.

Part II of this Article contends that hybrid IOT transactions are distinct from those entered into in the non-IOT setting, and given the complexities of such hybrid IOT transactions, the IOT will further exacerbate the problem of how to determine whether Article 2 applies to hybrid transactions. Part III applies the various existing approaches for evaluating Article 2's applicability to hybrid transactions to IOT hybrid contracts. This section argues that the predominant purpose and the gravamen of the claim tests are likely to be inadequate in the IOT era. This section also considers other sources of law that may be applicable to hybrid IOT transactions including the Magnuson-Moss Warranty-Federal Trade Improvement Act (Warranty Act)⁴⁸ and the Software Principles and highlights the limitations of these frameworks. Part IV proposes four solutions to resolve the hybrid transactions problem and addresses the potential critiques of each of these solutions. The Article ultimately calls for the adoption of a functionality approach.

46. See *infra* text accompanying note 124 (explaining how implied warranties are default obligations that may entitle buyers to compensation).

47. See U.C.C. § 9-102 (a)(44) (AM. LAW INST. & UNIF. LAW COMM'N 2010) (defining goods to include embedded computer programs and any supporting information).

48. Magnuson-Moss Warranty-Federal Trade Commission Improvement Act, Pub. L. No. 93-637, § 108(A), 88 Stat. 2183 (1975) (codified at 15 U.S.C. § 2301-2312).

II. *The Complexity of Hybrid IOT Transactions*

IOT transactions frequently involve an intricate provision of services, goods, and software that are in many instances distinct from the hybrid transactions of the pre-IOT era. The rapid expansion of the IOT and the complex nature of IOT transactions suggests that new frameworks for evaluating Article 2's role in hybrid transactions are needed.

A. *Mechanics of Hybrid IOT Transactions*

Contracts for the sale of goods are frequently accompanied by services.⁴⁹ In some instances, a retailer sells the goods to the buyer, but an independent third party or the seller provides installation services.⁵⁰ In other hybrid contracts, the seller provides the goods and labor needed to create the final product. For instance, the construction of a swimming pool involves the provision of supplies as well as services and labor needed to build the pool.⁵¹

However, the IOT transforms the interactions between buyers and sellers. The sale of a good can include not only a standard installation service contract but also additional continuous services and software—all of which are provided via interconnected devices.⁵² In the age of the IOT, companies are

49. See *Appliances Services*, BESTBUY.COM, <http://www.bestbuy.com/site/appliances-promotions/appliance-repair/pcmcat255100050002.c?id=pcmcat255100050002> (last visited Mar. 5, 2017) (“We’ll install your new major appliance and have it working when we leave.”) (on file with the Washington and Lee Law Review).

50. See Lisa Ryan, *Home Depot Fends Off Delivery Driver Wage Action*, LAW360 (July 11, 2014, 6:29 PM), <http://www.law360.com/articles/556582/home-depot-fends-off-delivery-driver-wage-action> (last visited Mar. 5, 2017) (reporting that Home Depot contracts delivery services through a third party) (on file with the Washington and Lee Law Review).

51. See DEPT OF CONSUMER AFFAIRS, CONTRACTORS STATE LICENSE BOARD, BEFORE YOU DIVE IN: A CONSUMER GUIDE TO SWIMMING POOL CONSTRUCTION (2014), <http://www.cslb.ca.gov/Resources/GuidesAndPublications/BeforeSwimmingPoolConstruction.pdf> (indicating that a contract must include description of the work and materials and equipment to be used).

52. See Elvy, *supra* note 19, at 841 (“These devices will be able to collect location and consumption rate data, among other things, about the consumer on

not only providing traditional installation services but they are continuing to provide new types of services and software even after the sale and installation of the device.⁵³ In this new setting, sellers are supplying much more than the labor needed to generate the final product.

Amazon's Dash Button, which is linked to a specific product, allows individuals to place orders automatically by clicking the Internet enabled device.⁵⁴ The sale of an Amazon Dash Button includes the purchase of the device and access to the accompanying product replacement service from Amazon.⁵⁵

Consider a consumer or a business that has purchased a Brother connected printer enabled with Amazon's dash replenishment service (DRS). Brother's DRS terms and conditions provide that buyers who elect to use its DRS enabled printers are given a license to use its software.⁵⁶ Amazon advertises DRS as a service that can be integrated into devices and it allows these connected devices to measure a purchaser's rate of consumption as well as place successive orders for new

behalf of the manufacturer and retailer.”).

53. *See id.* (detailing how a Brita device can automatically order replacement filters).

54. *See* Gordon Fletcher, *Amazon Dash is a First Step Towards an Internet of Things That Is Actually Useful*, CONVERSATION (Apr. 8, 2015, 1:31 AM), <http://theconversation.com/amazon-dash-is-a-first-step-towards-an-internet-of-things-that-is-actually-useful-39711> (last visited Mar. 5, 2017) (explaining how household goods can be ordered by scanning barcodes or utilizing speech recognition) (on file with the Washington and Lee Law Review); *see also* Brian Benchoff, *Inside the Amazon Dash Button*, HACKADAY (May 12, 2015), <http://hackaday.com/2015/05/12/inside-the-amazon-dash-button> (last visited Mar. 5, 2017) (describing the different product versions of Dash Button available) (on file with the Washington and Lee Law Review).

55. *See Amazon Offers Amazon Dash for \$5 to Premium Customers*, VENTURE CAP. POST (July 30, 2015, 6:26 PM), <http://www.vcpost.com/articles/81696/20150730/amazon-offers-dash-5-premium-customers.htm> (last visited Mar. 5, 2017) (offering the dash button for sale to Amazon premium customers for five dollars) (on file with the Washington and Lee Law Review).

56. *See Amazon Dash Replenishment Brother User Terms*, BROTHER-USA, <https://www.brother-usa.com/AmazonDash/terms.aspx> (last visited Mar. 5, 2017) (“Brother hereby grants you, free of charge, a non-exclusive and non-transferrable license to activate the Software in your Products . . .”) (on file with the Washington and Lee Law Review).

goods.⁵⁷ Amazon provides buyers with a separate terms of use for its DRS.⁵⁸ A buyer may have the ability to register or deregister the IOT device with DRS.⁵⁹ What appears to simply be the sale of a good—the printer—involves the provision of an ongoing service for subsequent purchases of printer ink without human intervention and a combination of software and hardware that measures the amount of printer ink being used by the purchaser, and collects and reports data about the device and the purchaser to the manufacturer or retailer. Thus, whenever a DRS enabled IOT device places an order for consumable supplies, the owner of the device will be purchasing goods while simultaneously using a product ordering service and accompanying software.⁶⁰

Admittedly, the combination of hardware and software is not a new development.⁶¹ IOT devices are embedded with high-velocity computer programs that are connected to

57. See *id.* (exchanging service-related information with makers of third party devices used); see also *Conditions of Use*, AMAZON, <http://www.amazon.com/gp/help/customer/display.html?nodeId=508088> (last updated Jun. 21, 2016) (last visited Mar. 5, 2017) (“When you use the Amazon Software, you may also be using the services of one or more third parties, such as a wireless carrier or a mobile platform provider.”) (on file with the Washington and Lee Law Review). See generally *Amazon Dash Replenishment Terms of Use*, AMAZON, <https://www.amazon.com/gp/help/customer/display.html?nodeId=201730770> (last updated Mar. 3, 2016) (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

58. See *Amazon Dash Replenishment Terms of Use*, *supra* note 57 (“By using Amazon Dash Replenishment, you agree to be bound by the terms of this Agreement. If you do not accept the terms of this Agreement, then you may not use Amazon Dash Replenishment.”) (on file with the Washington and Lee Law Review).

59. See *id.* (“LWA [Login With Amazon] allows customers to use their Amazon account credentials to register for DRS.”).

60. See Elvy, *supra* note 19, at 841 (detailing digital tracking technology embedded within IOT devices that permits automatic ordering).

61. See Jeff Nicholson, *First Take: Amazon Dash Buttons. The Internet of Things (IoT) takes a Big Step Forward*, CUSTOMER THINK (Apr. 1, 2015), <http://customerthink.com/first-take-amazon-dash-buttons-the-internet-of-things-iot-takes-a-big-step-forward/> (last visited Mar. 5, 2017) (“[T]he concept here is not new . . . due credit must go to the renowned example of Red Tomato Pizza which allowed . . . members to order a pizza with the click of a refrigerator magnet button.”) (on file with the Washington and Lee Law Review).

traditional networks, cloud or fog computing.⁶² This connection increases the capabilities of IOT devices and makes them significantly more powerful than traditional goods that contain a basic combination of hardware and software.⁶³

In the IOT setting, software and related services, such as mobile applications, play a central role in the operations of goods, unlike earlier generations of goods.⁶⁴ In fact, IOT devices are software-dominant products.⁶⁵ The unique combination of hardware, software, and services allows IOT devices to transmit data to a company about device errors, malfunctions, and the purchaser's rate of consumption, among other things.⁶⁶ It is estimated that by 2018 IOT devices will "generate more than 400 zettabytes of data—or the rough equivalent of all the data created from the dawn of the written word to the dawn of the Internet."⁶⁷

A buyer may purchase a product enabled with DRS from a retailer other than Amazon. This retailer may then offer installation services through an independent third party company while Amazon provides its replacement services and the product manufacturer provides software updates that allow the device to function.⁶⁸ In such an instance, installation services are being provided by a third party company or the

62. See Elvy, *supra* note 19, at 854 ("IOT robotic devices will be powered by the Internet and will be able to share data between devices, cloud software, and on-site infrastructure.").

63. See *id.* (noting that IOT robotic devices will do more than simply enter into transactions based on preexisting agreements, or make preprogrammed choices).

64. See *id.* at 853 ("With the DRS, consumers 'don't have to do anything—they can simply rely on the connected device to automatically reorder the consumables to keep their homes running smoothly.'").

65. See *id.* at 846 ("Approximately ninety percent of companies expect to access and store data generated by IOT robots via cloud infrastructure and software rather than through onsite infrastructure.").

66. See *id.* at 841 (explaining how the readable element in the packaging is transforming the marketing industry).

67. Terrell McSweeney, Commissioner, Fed. Trade Comm'n, Remarks to the Chamber of Commerce at TecNation: Meeting the Challenges of the Digital Age (Sep. 20, 2016).

68. See *Appliances Services*, *supra* note 49 (indicating that delivery may be performed by a third party company).

initial retailer, but Amazon continues to provide an ongoing service for the purchase and sale of new products.⁶⁹ Further, complicating such transactions is the ability of independent sellers to sell goods on Amazon directly to buyers.⁷⁰ The buyer may also be granted a license to use the manufacturer's software. A buyer of an IOT device may be subject to three separate contracts and potentially multiple sources of law: (1) an end user licensing agreement (EULA) subject to intellectual property law, the common-law or potentially the Uniform Computer Information Transactions Act (UCITA) for the software that allows the IOT device to function;⁷¹ (2) a contract subject to Article 2 or the common-law, which is provided by the manufacturer or retailer for the sale and purchase of the IOT device—this contract may include a limited warranty that covers the device but excludes software and services—and (3) a licensing agreement for the use of the company's product ordering, monitoring, or other application services.⁷²

One could view an IOT transaction involving goods, DRS, and software as separate transactions: one in which a buyer purchases the device from the manufacturer or retailer and obtains a license to use the accompanying software from the manufacturer, and another transaction in which a buyer registers the device with Amazon to use DRS. However, the first

69. See Elvy, *supra* note 19, at 895 (“Manufacturers that embed Amazon’s DRS into their products . . . could have unparalleled access to data about how consumers use such products once the product is in a consumer’s home.”).

70. In such cases Amazon provides an A–Z Guarantee: “[W]e guarantee purchases from third party sellers when payment is made via the Amazon.com website or when buyers use Amazon Payments for qualified purchases on third party websites. The condition of the item [purchased] and its timely delivery are guaranteed under the Amazon A-to-Z Guarantee.” *Help & Customer Service: About A-to-z Guarantee*, AMAZON, <http://www.amazon.com/gp/help/customer/display.html?nodeId=200783670> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

71. See Florencia Marotta-Wurgler & Robert Taylor, *Set in Stone? Change and Innovation in Consumer Standard-Form Contracts*, 88 N.Y.U. L. REV. 240, 250 (2013) (suggesting that EULAs may be subject to UCITA).

72. See *Amazon Dash Replenishment Terms of Use*, *supra* note 57 (explaining that the use of third party Service Enabled Devices are subject to the original Amazon sales agreement).

transaction remains a hybrid transaction because it involves the simultaneous provision of goods and software.⁷³ The second transaction involves the use of software embedded within goods and services. Even if the services and software are provided at different times and by different parties, both are needed in order for the device to achieve full functionality as advertised by the manufacturer or retailer.

Where the manufacturer and retailer are the same entity, and provide all of the services and software, it becomes more difficult to contend that the transactions should be evaluated separately. For instance, the purchase of an IOT thermostat from Nest, which monitors users' daily movements and adjusts the temperature in a user's home, includes not only the physical device and accompanying software but also a monthly energy report.⁷⁴ The report summarizes the heating and cooling usage of buyers who own a Wi-Fi connected Nest Learning Thermostat.⁷⁵ Nest provides various services that work together with its IOT devices, such as a Nest user account website, mobile applications and subscription services all of which allow users to control and operate their devices.⁷⁶ Nest also supplies purchasers with information about authorized third party companies that offer standard installation services for Nest IOT devices.⁷⁷ Nest provides three separate agreements that govern

73. See Braucher, *supra* note 34, at 246 (describing hybrid transactions as non-sale transactions).

74. See *Learn More About the Nest Home Report*, NEST SUPPORT, <https://nest.com/support/article/About-the-Nest-Home-Report> (last visited Mar. 5, 2017) (detailing the Nest Home Report that provides comparative usage data and tips on how to save energy) (on file with the Washington and Lee Law Review).

75. See *Why Haven't I Received My Nest Home Report?*, NEST SUPPORT, <https://nest.com/support/article/Why-haven-t-I-received-my-Nest-Home-Report> (last updated Dec. 22, 2016) (last visited Mar. 5, 2017) (troubleshooting steps to successfully receive Nest Home Reports) (on file with the Washington and Lee Law Review).

76. See *Terms of Service*, NEST, <https://nest.com/legal/terms-of-service/> (last updated Mar. 10, 2016) (last visited Mar. 5, 2017) (noting that some Nest products and services can also be used in ways that integrate with third party products and services) (on file with the Washington and Lee Law Review).

77. See *How Do I Arrange for Professional Installation Through My Nest Retailer?*, NEST, <https://nest.com/uk/support/article/How-do-I-arrange-for->

transactions involving their devices: (1) an EULA for the software provided in connection with their devices,⁷⁸ (2) terms and conditions that apply to the sale of the device,⁷⁹ and (3) a service agreement that governs accompanying services.⁸⁰

Viewing a hybrid IOT transaction as involving separate and distinct contracts for goods, services, and software is highly problematic where a manufacturer elects to terminate the services that support the device's operations. Unless companies elect to provide adequate compensation to buyers when they terminate services for IOT devices, buyers may be left with IOT devices that simply do not function. The service agreement may also provide buyers with no recourse where service is interrupted or suspended, which could render the device useless during that period. As the IOT evolves, the services provided by companies in support of IOT devices may become even more critical to the functioning and performance of the device, but such services are not typically covered by warranties. If the services and software provided in connection with the sale of a device are central to the operations of the device and those services are terminated or interrupted, Article 2 should govern the resulting dispute.

B. Distinctions Between IOT and Other Hybrid Transactions

IOT hybrid agreements are unlike other hybrid transactions in several ways. First, these transactions are different from the standard service contracts consumers or businesses may purchase in connection with the sale of goods. Business and home service contracts are typically warranty contracts that

professional-installation-through-my-Nest-retailer (last visited Mar. 5, 2017) (explaining the various installation options available from Nest retailers) (on file with the Washington and Lee Law Review).

78. *End User License Agreement*, NEST, <https://nest.com/legal/eula/> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

79. *Sales Terms*, NEST, <https://nest.com/legal/sales-terms/> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review); *Limited Warranty Thermostat*, Nest, <https://nest.com/legal/warranty/thermostat/> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

80. *Terms of Service*, *supra* note 76.

extend the life of existing warranties or obligate a company to repair or replace defective parts.⁸¹ However, IOT services, such as DRS, are not currently offered to protect buyers in the event the device malfunctions. Rather, IOT services, software and devices work together to measure consumption rates, collect, and transmit data about owners to companies, automatically order goods, and allow owners to remotely control multiple devices, among other things.⁸² Of course, standard service contracts that provide guarantees for defective parts may also be offered by companies in connection with the provision of IOT devices. This would increase the types of services being offered in an IOT transaction. Such a transaction would involve both new IOT services, such as product ordering and mobile application services, as well as a standard service contract. Additionally, companies may ultimately expand and create new types of services that are provided through IOT devices.

While companies have used ordering and subscription services for years to increase sales,⁸³ IOT services are distinct

81. Some states may also regulate the provision of certain service contracts via the adoption of the Model Services Contract Act of the National Association of Insurance Commissioners. See SERV. CONTRACTS MODEL ACT (NAT'L ASS'N INS. COMM'RS 1997), <http://www.naic.org/store/free/MDL-685.pdf> (providing a model statute for the regulation of service contracts); see also ALA. CODE §§ 8-32-1 to -12. (2016) (creating a framework to regulate service contracts); Ariz. Rev. Stat. §§ 20-1095 to -1095.10 (2016) (regulating contracts offered by service companies); ARK. CODE ANN. §§ 4-114-101 to -112, 4-90-501 to -512 (2016) (creating a framework for regulating service contracts and offering consumer protections); CAL. BUS. & PROF. CODE §§ 9855 to 9855.9, 12800–12816, 12740–12767 (2016) (concerning motor vehicle and residential insurance); HAW. REV. STAT. §§ 481X-1 to -12 (2016) (regulating service contracts); IDAHO CODE §§ 41-114A, 49-2801 to -3715 (2016) (concerning motor vehicle insurance); 215 ILL. COMP. STAT. 152/1 to 152/99 (2016) (regulating service contracts); IOWA CODE §§ 523C.1–.25, 516E.1–.21 (2016) (relating to residential and motor vehicle insurance, respectively).

82. See *Get Started With Dash Replenishment*, <https://developer.amazon.com/dash-replenishment-service/getting-started>, AMAZON DEVELOPER (last visited Mar. 5, 2017) (providing an overview of DRS services and functions) (on file with the Washington and Lee Law Review).

83. See Michael Lev-Ram, *It's a Subscription Economy and You're Just Living in It*, FORTUNE (June 6, 2014, 6:42 AM), <http://fortune.com/2014/06/06/welcome-to-the-subscription-economy> (last visited Mar. 5, 2017) (“It’s actually not that new: Businesses have been selling monthly subscriptions for all sorts of goods and services for years—magazines like Fortune come to mind.”) (on file with the Washington and Lee Law Review).

from these types of service options, which have previously accompanied the sale of goods. Historically, a buyer was able to enter into a contract for the sale of a static device, such as a thermostat, via a subscription or ordering service—but the usefulness of such a thermostat to the buyer did not depend on the subscription service provided by the company.⁸⁴ The functionality of the thermostat was not connected to, and did not rely, on the ordering or subscription service.⁸⁵ In contrast, in the IOT setting, buyers likely choose to purchase IOT devices, such as a Nest Learning Thermostat or a Brother DRS printer, over a non-IOT printer or thermostat, because of the smart home capabilities of the IOT version of these goods, and the services advertised by companies as being necessary for the buyer to enjoy the full array of benefits provided by these IOT devices.⁸⁶ A buyer may purchase a Nest Learning Thermostat because of the useful energy reports and the ability to control the device using the company's mobile application.⁸⁷ A buyer may elect to purchase a DRS-enabled washer because the device will be able to dispense the amount of detergent needed to do a load of laundry, measure consumable usage, and automatically place subsequent orders for detergent using the accompanying service.⁸⁸ Subscription and product ordering services are no

84. See *Internet of Things: Science Fiction or Business Fact?*, 2014 HARV. BUS. REV. 1, 3 (Sept. 2014), http://hbr.org/resources/pdfs/comm/verizon/18980_HBR_Verizon_IoT_Nov_14.pdf (providing an overview of the Internet of Things and noting potential challenges inherent to shifting from a products-based business to a service-based or hybrid business).

85. *Id.*

86. See *Works With Nest*, NEST, <https://nest.com/works-with-nest> (last visited Mar. 5, 2017) (demonstrating the interdependency of Nest products and services) (on file with the Washington and Lee Law Review); see also *CONNECT.PRINT.SHARE.*, BROTHER, <http://www.brother-usa.com/connect/mobile> (last visited Mar. 5, 2017) (demonstrating the interdependency of Brother products and services) (on file with the Washington and Lee Law Review).

87. See *Nest App*, NEST, <https://nest.com/app> (last visited Mar. 5, 2017) (advertising the features available through use of Nest's mobile application) (on file with the Washington and Lee Law Review).

88. See *First Amazon Dash Replenishment Devices Now Available*, BUS. WIRE (Jan. 19, 2016, 9:00 AM), <http://www.businesswire.com/news/home/20160119005749/en/Amazon-Dash-Replenishment-Devices> (last visited Mar. 5, 2017) ("GE's washer with Smart Dispense technology stores detergent and automatically dispenses the right amount for each load so customers don't have

longer stand alone items or offers but are very much connected to, and supplied directly through IOT devices.⁸⁹

Consider that the defining feature of an IOT sex toy manufactured by Standard Innovation Corporation is a mobile application that allows owners of the smart device to control the device “from near or far, letting a user change vibration modes from their phone or allow a far-flung partner to take the reins”⁹⁰ Similarly, the valuable video feeds and clips generated by a Nest Cam are only available via Nest’s mobile application and website.⁹¹ While security cameras and video feeds are not new, IOT security cameras permit owners to remotely view security feeds and control the devices through a mobile application or a website without a physical video system.⁹² While not all IOT devices can be accessed and controlled by a mobile application, the range of operations of an IOT device is very much dependent on the services and software provided by companies.

The failure of IOT manufacturers to properly maintain and monitor a device and the accompanying software and services may have dire consequences for consumers. For example, a smart Dexcom glucose monitoring device that allows owners to continuously and remotely track and share glucose levels, failed to alert a consumer of his low blood sugar levels, which resulted

to worry about it. With Dash Replenishment, customers use the associated app to set their preferred preorder level and Amazon delivers detergent when supply is running low.”) (on file with the Washington and Lee Law Review).

89. See *supra* Part II.A (discussing DRS devices and services).

90. Shayna Possess, *Vibrator Gets Too Intimate by Tracking Usage Infos, Suit Says*, LAW360 (Sept. 15, 2016, 3:57 PM), <http://www.law360.com/articles/840299/vibrator-gets-too-intimate-by-tracking-usage-info-suit-says> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

91. See *FAQs About Moving From the Dropcam App to the Nest App*, NEST, <https://www.nest.com/support/article/FAQs-about-moving-from-the-Dropcam-app-to-the-Nest-app> (last visited Mar. 5, 2017) (answering general questions consumers may have concerning the Nest application’s functionality) (on file with the Washington and Lee Law Review).

92. See Megan Wollerton, *Nest Cam Outdoor Review*, CNET (Sept. 15, 2016), <https://www.cnet.com/products/nest-cam-outdoor/review> (reviewing the function and features of Nest’s outdoor camera) (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

in a car crash after the consumer lost consciousness while driving.⁹³

Unlike many software hybrid transactions that involve the creation of software programs tailored to the needs of a buyer, in many consumer IOT hybrid transactions a buyer purchases devices that are embedded with pre-existing standardized software and accompanied by software updates.⁹⁴ Of course, the monetization of software in the IOT setting could result in consumers working with IOT companies to customize their IOT devices. Additionally, a scenario could easily be envisioned where a company purchases an IOT manufacturing device and requires the seller to customize the accompanying software, hardware, and services to suit the company's needs.

Given the frequency with which devices and servers are hacked,⁹⁵ the software contained in many IOT devices will likely become vulnerable to intrusion over time, requiring IOT manufacturers to offer software and security upgrades throughout the life of the device. For instance, in 2016, hackers exposed serious vulnerabilities in Tesla's Model S sedan which allowed them to remotely open car trunks, manipulate car brakes and adjust the seating.⁹⁶ Nest software updates allow

93. See Emily Field, *Blood Sugar Monitor Maker Hit with Suit Over Car Crash*, LAW360 (Aug. 31, 2016, 4:59 PM), <http://www.law360.com/articles/834866/blood-sugar-monitor-maker-hit-with-suit-over-car-crash> (last visited Mar. 5, 2017) (detailing the factual background of the consumer's legal action against Dexcom) (on file with the Washington and Lee Law Review). The Federal Drug Administration had previously taken steps to attempt to address consumer concerns with Dexcom's devices. *Id.*

94. For example, Nest's outdoor camera and accompanying app provide cloud storage for up to three hours of video content. See Wollerton, *supra* note 92 (explaining the capabilities of the Nest system).

95. See David Maman, *Database Hacking: The Year That Was*, HELP NET SEC. (Dec. 31, 2012), <https://www.helpnetsecurity.com/2012/12/31/database-hacking-the-year-that-was> (last visited Mar. 5, 2017) ("Database breaches happen every day—internally, from dishonest employees and subcontractors, to external sources such as hackers using SQL injections, worms infecting public web sites, massive phishing attacks, and targeted attacks on financial institutions and defense organizations.") (on file with the Washington and Lee Law Review).

96. See Rob Price, *Car Hackers Found a Way to Trigger a Tesla's Brakes from Miles away*, BUS. INSIDER (Sept. 20, 2016), <http://www.businessinsider.com/car-hackers-trigger-tesla-model-s-brakes-unlock-doors-adjust-seats-tencent-keen-security-lab-2016-9> (last visited Mar. 5, 2017) (explaining how car hackers were

Nest to send messages to an owner's phone when temperature fluctuations may lead to frozen pipes.⁹⁷ Owners of Nest Protect can view smoke and carbon monoxide alarms on the Nest Learning Thermostat and multiple Nest thermostats now have the capacity to work together to save energy as a result of recent software updates.⁹⁸ The recently launched Nest Cam Outdoor provides notifications to an owner's smartphone when it detects suspicious activity, records the event, and sends the video directly to a Nest cloud-based server.⁹⁹

Although IOT devices may receive software updates from manufacturers in the same way that a buyer may obtain software updates in connection with the sale of a computer,¹⁰⁰ IOT devices—unlike these traditional products—have the capacity to independently track consumption rates and order goods via the ongoing services provided by a manufacturer or third party company.¹⁰¹ A computer may continue to function

able to override the Tesla's autopilot system) (on file with the Washington and Lee Law Review). In response, Tesla rolled out a security patch to fix the problem. *See id.* (explaining Tesla's response to rectify this serious error).

97. *See* Kellex, *Nest Introduces New Protect and Cam, Updates Software for Thermostat and Apps*, DROID LIFE (June 17, 2015), <http://www.droid-life.com/2015/06/17/nest-introduces-new-protect-and-cam-updates-software-for-thermostat-and-apps> (last visited Mar. 5, 2017) ("The best-selling *Nest Learning Thermostat* is getting even better, now notifying customers when temperatures drop to help avoid frozen pipes and adding new integrations with other Nest products.") (on file with the Washington and Lee Law Review).

98. *Id.*

99. *See* Horia Ungureanu, *Nest Finally Launches an Outdoor Security Camera: Meet The \$199 Nest Cam Outdoor, On Preorder Now*, TECH TIMES (July 14, 2016, 10:41 AM), <http://www.techtimes.com/articles/169880/20160714/nest-finally-launches-an-outdoor-security-camera-meet-the-199-nest-cam-outdoor-on-preorder-now-video.htm> (last visited Mar. 5, 2017) (detailing the features and functions of Nest's outdoor security camera) (on file with the Washington and Lee Law Review).

100. For example, Microsoft's Windows 10 operating system automatically delivers software updates to personal computers. *See* Sarah Jacobsson Purewal, *Stop Windows 10 From Automatically Updating Your PC*, CNET (May 18, 2016, 12:20 PM), <https://www.cnet.com/how-to/stop-windows-10-from-automatically-updating-your-pc> (last visited Mar. 5, 2017) ("Windows 10 automatically checks for, downloads and installs new updates to your PC—whether you like it or not.") (on file with the Washington and Lee Law Review).

101. For instance, Amazon's DRS utilizes these IOT device features to take shipping orders automatically. *See Get Started with Dash Replenishment*,

with the software that was pre-installed by the company upon purchase, and a buyer does not always need to rely on software updates or services from the manufacturer or retailer.¹⁰² In contrast, the functionality of IOT devices depends significantly on the services and software provided by manufacturers and retailers. In some instances, buyers are required to consent to automatic software updates to their Wi-Fi connected IOT devices.¹⁰³ If a purchaser objects to their IOT device receiving software updates, their only remedy is to stop using the device.¹⁰⁴

While there may be some similarities between traditional hybrid transactions involving the sale of goods, software, and services, IOT hybrid transactions involve a multifarious array of new and ongoing services and software that may be provided by multiple parties. The new types of services and software that are expected to be provided in IOT transactions, along with the possibility that companies may continue to provide standard services, including installation services, will generate even more elaborate hybrid transactions.¹⁰⁵ This increased level of complexity provides a strong justification for the development of new approaches in this area.

AMAZON DEVELOPER, <https://developer.amazon.com/dash-replenishment-service/getting-started> (last visited Mar. 5, 2017) (providing an overview of the Dash Replenishment Service) (on file with the Washington and Lee Law Review).

102. See Tim Fisher, *Windows Updates and Patch Tuesday FAQ*, LIVEWIRE, <https://www.lifewire.com/windows-updates-patch-tuesday-faq-2625777> (last updated Apr. 1, 2016) (last visited Mar. 5, 2017) (noting that software updates are not necessary for Windows to function) (on file with the Washington and Lee Law Review).

103. See, e.g., *End User License Agreement*, *supra* note 78 (noting that by using Nest devices a buyer consents automatically to software updates).

104. See *Terms of Service*, *supra* note 76 (“You consent to this automatic update. If you do not want such Updates, your remedy is to terminate your Account and stop using the Services and the Product.”).

105. Some tech and marketing consultants have already taken notice of IOT’s potential, especially in private residences. See, e.g., Joe Fletcher, *Bundling Services in IoT (Part II)*, MEDIUM (July 27, 2016), <https://medium.com/@joefletcher/bundling-services-in-iot-part-ii-40f4ab92419c#.jb1hdv93f> (last visited Mar. 5, 2017) (calling for third party companies to offer hybrid deals) (on file with the Washington and Lee Law Review).

III. The Inadequacy of Current Approaches in the IOT Era

Article 2's applicability to transactions involving goods and non-goods has long been a vexing problem. This section highlights the inadequacies of the different approaches offered to address the hybrid transactions problem and evaluates the potential role of common-law warranties, the Warranty Act, UCITA, and the Software Principles in ameliorating the concerns raised by such transactions. Common-law warranties are unlikely to be widely applied to IOT transactions and while the Warranty Act has promise, its ability to protect consumers has been limited in a number of areas. The Software Principles suffer from several limitations, some of which are similar to the deficiencies found in the current approaches used to address hybrid transactions. UCITA has not been widely accepted by states.

A. Services and Goods under Article 2

To encourage the adoption of a uniform law on commercial transactions, Karl Llewellyn contended in 1939 that American sales law was inadequate for the industrial economy.¹⁰⁶ Today, we have transitioned from the industrial era to an information, service and sharing economy.¹⁰⁷ The IOT is expected to revolutionize the information economy.¹⁰⁸ Article 2 and its definition of goods were adopted to address transactions where the sale of movable goods was the essence of the transaction. Section 2-102 of the UCC provides that Article 2 applies to

106. See generally Llewellyn, *supra* note 2, at 876.

107. See Lorin Brennan, *Why Article 2 Cannot Apply to Software Transactions*, 38 DUQ. L. REV. 459, 461 (2000) ("We are undergoing another change today It is the transition from an industrial to an information economy.").

108. See Susan Fourtané, *IoT Revolution: Is the Enterprise Ready?*, INFO. WK. (Mar. 27, 2015, 8:05 AM), <http://www.informationweek.com/strategic-cio/it-strategy/iot-revolution-is-the-enterprise-ready/a/d-id/1319636> (last visited Mar. 5, 2017) ("There is little doubt the Internet of Things revolution is coming, and it will fundamentally change the way people interact with different devices.") (on file with the Washington and Lee Law Review).

transactions in goods.¹⁰⁹ Subject to a few exceptions, goods are defined as all things moveable at the time of identification to the contract.¹¹⁰ The predominant purpose and the gravamen of the claim tests have been offered by commentators as effective solutions for evaluating Article 2's applicability to transactions involving the sale of goods and services.¹¹¹ This Subpart will explain each of these tests and apply them to IOT transactions and argues that these tests are insufficient for the IOT era.

1. *Predominant Purpose Test*

To evaluate whether Article 2 applies to a hybrid transaction, most jurisdictions have adopted the predominant purpose test.¹¹² Courts assess whether the predominant purpose of the transaction is for the provision of goods or services.¹¹³ Article 2 will apply only where the transaction is predominantly for the provision of goods.¹¹⁴ If the service aspect of the contract predominates then the warranties of quality under Article 2 are likely not applicable.¹¹⁵

109. U.C.C. § 2-102 (AM. LAW INST. & UNIF. LAW COMM'N 2002).

110. *Id.* § 2-105.

111. This Article explores the courts' use of the predominant purpose test in the following subsection. *Infra* Part III.A.1. The article will subsequently discuss use of the gravamen of the claim test. *Infra* Part III.A.2.

112. See Abby J. Hardwick, Note, *Amending the Uniform Commercial Code: How Will a Change in Scope Alter the Concept of Goods?*, 82 WASH. U. L.Q. 275, 280 (2004) ("The test most commonly used by the courts was the predominant purpose test."); see also E. ALLAN FARNSWORTH, FARNSWORTH ON CONTRACTS § 1.9, at 44 (3d ed. 2004) ("Courts usually determine whether a transaction is one in goods, services, or land by looking for the 'predominant factor' of the contract.").

113. See *Bonebrake v. Cox*, 499 F.2d 951, 960 (8th Cir. 1974) ("The test for inclusion or exclusion [in the U.C.C.] is not whether they are mixed, but, granting that they are mixed, whether their predominant factor, their thrust, their purpose, reasonably stated, is the rendition of service, with goods incidentally involved . . .").

114. *Id.*

115. See *id.* at 958 ("[U.C.C. § 2-102] is divided into two parts, the first affirmative, defining the scope and reach of Article 2, the second negative, excluding certain transactions. To come within the affirmative section, the articles must be movable, and the movability must occur at the time of identification to the contract.").

Courts often use different factors to assess whether the predominant purpose of the transaction is for the sale of goods or services. For instance, in *Colorado Carpet Installation, Inc. v. Palermo*,¹¹⁶ the court held that in evaluating the circumstances surrounding the contract and its performance, the following factors should be used: the contract language; whether the contract provides an overall price or separate prices for goods and labor; the ratio of the costs of the goods to the total contract price; and the nature and reasonableness of the purchaser's contractual expectations of acquiring a property interest in the goods.¹¹⁷

A Delaware court noted that the factual circumstances surrounding the negotiation, formation, and contemplated performance of the contract should be considered; however, "if the cause of action centers exclusively on the materials portion or the services portion of the contract, the determination may rest upon that fact."¹¹⁸ In applying the predominant purpose test, the

116. 668 P.2d 1384 (Colo. 1983).

117. See *id.* at 1388–89 (listing factors used to apply the predominant purpose test); see also *Stafford v. Int'l Harvester Co.*, 668 F.2d 142, 147 (2d Cir. 1981) ("[T]he underlying nature of a hybrid transaction is determined by reference to the purpose with which the customer contracted with the defendant . . ."); *Neibarger v. Universal Coops., Inc.*, 486 N.W.2d 612, 622 (Mich. 1992) ("If the purchaser's ultimate goal is to acquire a product, the contract should be considered a transaction in goods Conversely, if the purchaser's ultimate goal is to procure a service, the contract is not governed by the UCC, even though goods are incidentally required in the provision of this service."). This focus on the purchaser's intent presumes that the services and goods can be easily separated and that the service does not impact functionality of the goods. This becomes problematic in the IOT setting where the operations of the device are dependent on the service and software provided by the manufacturer or retailer and the services are no longer incidental to the device. Additionally, in some instances, courts have also evaluated whether the final product produced in a hybrid transaction is movable, thereby, meeting the definition of goods under Article 2. See generally *Meyers v. Henderson Constr. Co.* 370 A.2d 547 (N.J. Super. Ct. App. Div. 1977) (finding that the predominant purpose of the transaction was for the provision of prefabricated but disassembled doors); *Lake Wales Publ'g Co. v. Florida Visitor Inc.*, 335 So. 2d 335 (Fla. Dist. Ct. App. 1976) (finding that the production of printed pamphlets were goods subject to the UCC). The functionality approach advocated for in Part IV.B of this Article evaluates much more than whether the finished product sold to a buyer is movable. *Infra* Part IV.B. The functionality approach also addresses the extent to which ongoing services and software are needed for the product to function.

118. See *Glover Sch. & Office Equip. Co. v. Dave Hall, Inc.*, 372 A.2d 221, 223

Fourth Circuit has considered the nature of a supplier's business in addition to the contract language and the value of the materials.¹¹⁹ Moreover, even when courts identify the specific factors to be considered when applying the predominant purpose test, courts rarely provide a clear analysis that applies the factors to the facts of the case.¹²⁰ Instead, courts often simply "state the facts and then declare an answer."¹²¹ Application of the predominant purpose test requires courts to engage in a retrospective analysis regarding the predominating purpose of a hybrid transaction.¹²²

Given the various factors used by courts in applying the predominant purpose test it is not surprising that different courts applying this test to similar facts have reached opposite conclusions.¹²³ For instance, disputes involving the sale and installation of swimming pools, flooring, alarm systems, and air conditioning have led to conflicting case law.¹²⁴ In *Baker v.*

(Del. Super. Ct. 1977) (examining the nature of a transaction to supply and install schoolhouse equipment and noting that the price of the goods in comparison to the services may also be relevant).

119. See *Coakley & Williams, Inc. v. Shatterproof Glass Corp.*, 706 F.2d 456, 460 (4th Cir. 1983) ("They emphasize, in particular, three aspects which may, or may not, constitute indicia of the nature of the contract: (1) the language of the contract, (2) the nature of the business of the supplier, and (3) the intrinsic worth of the materials involved.").

120. See LINDA J. RUSCH & STEPHEN L. SEPINUCK, *COMMERCIAL LAW: PROBLEMS AND MATERIALS ON SALES AND PAYMENTS* 24 (2012) (discussing application of the predominant purpose test).

121. *Id.*

122. See Laura McNeill Hutcheson, *The Exclusion of Embedded Software and Merely Incidental Information from the Scope of Article 2B: Proposals for New Language Based on Policy and Interpretation*, 13 BERKELEY TECH. L. J. 977, 978 n.8 (1998) (discussing an amendment to the U.C.C. which would address software licensing and electronic contracts).

123. HAWKLAND, *supra* note 8, § 2-102 (noting that "the application of the predominate purpose test is inherently a factual inquiry where similar circumstances can result in divergent decisions. For example, using the predominate purpose test, courts sometimes conclude that a building contract is governed by Article 2, and other courts conclude that Article 2 does not apply.").

124. See *generally* NAT'L CONSUMER LAW CTR., *THE CONSUMER CREDIT AND SALES LEGAL PRACTICE SERIES: SALES OF GOODS AND SERVICES* 161 (2d ed. 1989); Jesse M. Brush, *Mixed Contracts and the UCC: A Proposal for Uniform Penalty Default to Protect Consumers* 11–13 (Student Scholarship Papers, Working Paper No. 47, 2007) (on file with author). Compare *Riffe v. Black*, 548 S.W.2d 175, 176–

Compton,¹²⁵ the court found that Article 2 applied to a contract for the sale and installation of furnaces, air conditioners, and water heaters in a building as the equipment represented a majority of the purchase price and the services were incidental to the sale of the goods.¹²⁶ In contrast, in *Mingledorff's, Inc., v. Hicks*,¹²⁷ the court determined that a contract for the sale and installation of heating and air conditioning systems in an apartment complex was not subject to Article 2 as the equipment and material furnished were incidental to the contract.¹²⁸

The Fourth Circuit has acknowledged that there is a “welter of [hybrid transactions] cases reaching varying results depending on the considerations deemed to predominate in each particular case.”¹²⁹ The predominant purpose test along with the various factors used by courts applying this test has created a lack of uniformity and clarity in decisions addressing the applicability of Article 2 to hybrid transactions, which contradicts the stated goals of the UCC.¹³⁰

78 (Ky. 1977) (affirming the trial court’s finding that implied warranties existed in the sale and installation of a swimming pool), *with* *Gulash v. Stylarama*, 364 A.2d 1221, 1223–24 (Conn. C.P. 1975) (finding that a contract to sell and install an aboveground swimming pool was not a sale of goods). In *Aluminum Co. of Am. v. Electro Flo Corp.*, which involved the design and production of flooring material, the Tenth Circuit held that Article 2 and an implied warranty applied to the transaction. 451 F.2d 1115, 1118 (10th Cir. 1971). In contrast, in *Ranger Constr. Co. v. Dixie Floor Co.*, the South Carolina federal district court held that a contract for the installation and sale of flooring was not subject to Article 2. 433 F. Supp. 442 (D.S.C. 1977).

125. 455 N.E.2d 382 (Ind. Ct. App. 1983).

126. *Id.* at 385–86; *see also* *Aluminum Co. of Am. v. Electro Flo Corp.*, 451 F.2d 1115, 1118 (10th Cir. 1971) (“We hold that the transaction between Alcoa and Electro Flo, while it involve some engineering and design aspects, was in essence a sale of goods.”).

127. 209 S.E.2d 661 (1974).

128. *Id.* at 662; *see also* *Ranger Constr. Co. v. Dixie Floor Co., Inc.*, 433 F. Supp. 442, 445 (D.S.C. 1977) (“[I]t is only logical to conclude that the contract in dispute in this case is . . . a contract for the performance of services with the sale of the goods necessary to perform those services being incidental to the service contract. Therefore, the [U.C.C.] would not be applicable in this case.”).

129. *Coakley & Williams, Inc. v. Shatterproof Glass Corp.*, 706 F.2d 456, 460 (4th Cir. 1983).

130. One of the UCC’s stated goals is “to simplify, clarify, and modernize the law governing commercial transactions.” U.C.C. § 1-103(a)(1) (AM. LAW INST. & UNIF. LAW COMM’N 2002).

Application of the predominant purpose test to IOT transactions may also lead to ambiguous or conflicting results. For example, consider a contract for the purchase of a Brother printer enabled with DRS. Is such a contract predominantly for the purchase of the printer? One could argue that a consumer or a business purchases a printer in order to use the product and DRS is incidental to such a transaction. However, DRS permits the printer to automatically reorder printer ink, which is also instrumental to the functioning of the printer. Of course, a buyer may ultimately elect not to use DRS to order printer ink, but a buyer's decision regarding the utilization of DRS after purchasing an IOT device is likely not relevant in assessing the predominant purpose of a transaction as this test focuses on the purpose of the transaction at the time the parties entered into the contract. The predominant purpose test also presumes that a court can accurately assess the objective of a transaction at the time of contracting.¹³¹ The parties' agreement may reference a stated purpose but a party may have a hidden or alternate agenda.

The usefulness of IOT smart home devices, such as the Nest Learning Thermostat, Nest Cam, and Nest Protect, depends heavily on the services being provided by the company. A buyer who owns all three of Nest's products may control and access these devices through the Nest application.¹³² While the predominant purpose of such a transaction may appear to be the sale of the device, as I have noted in Part II above, these products may be attractive to buyers because of the services provided in connection with the device. One could argue that the online services provided are even more valuable to the buyer than the device. Such a transaction could easily be categorized as a transaction whose predominant purpose is for the provision

131. See *Bonebrake v. Cox*, 499 F.2d 951, 960 (8th Cir. 1974) ("The test for inclusion or exclusion [in the U.C.C.] is not whether they are mixed, but, granting that they are mixed, whether their predominant factor, their thrust, their *purpose*, reasonably stated, is the rendition of service, with goods incidentally involved" (emphasis added)).

132. See *Meet The All-New Nest Protect*, NEST, <https://nest.com/smoke-co-alarm/meet-nest-protect> (last visited Mar. 5, 2017) (providing an overview of Nest products) (on file with the Washington and Lee Law Review).

of services rather than goods, thereby removing the transaction from Article 2's coverage.

Article 2's definition of goods was drafted during a time in which goods may have held more value for a buyer than any accompanying service provided by the seller.¹³³ In IOT hybrid transactions, the essence of the transaction is not limited solely to the provision of the device; the services and software provided along with the IOT device are just as important to the buyer as the device itself.¹³⁴ Buyers have grown accustomed to receiving goods that are bundled with services and software. In fact, "the value of physical devices more and more is defined by the embedded software inside them or the control software that helps to manage them."¹³⁵ IOT devices cannot fully operate without the software and the services provided by the manufacturer or retailer, but the software and services that are provided may only be useful to the extent that the buyer has ownership of the device. Thus, one aspect of a hybrid IOT transaction may not predominate over another or alternatively, the provision of software and IOT services may be the predominant purpose of an IOT transaction.

Now suppose the buyer above who has purchased the Brother printer from Amazon is dissatisfied with DRS. If a court determines that Article 2 applies to the transaction under the predominant purpose test and the dispute is about the service

133. Article 2 was initially published in 1952, a time when the consumer finance industry grew as Americans sought to buy more consumer goods. See Jan Logemann, *Different Paths to Mass Consumption: Consumer Credit in the United States and West Germany During the 1950s and '60s*, 2008 J. Soc. HIST. 525 (noting that, in the post-World War II United States, consumer credit and consumer culture became the norm).

134. See Vincent Smyth, *2016 Trends: The Internet of Things and Software Monetisation*, IT PRO PORTAL (Dec. 31, 2015), <http://www.itproportal.com/2015/12/31/2016-trends-internet-of-things-software-monetisation> (last visited Mar. 5, 2017) ("In order to participate in this new industrial revolution . . . IoT makers are becoming software-centric. This is so because the value of physical devices more and more is defined by the embedded software inside them or the control software that helps to manage them.") (on file with the Washington and Lee Law Review).

135. See *id.* ("This is obvious when we consider our own smartphones and tablets—they're valuable to us because of the specific apps we each run on them that make them personal and productive for our own purposes.").

and the printer—for instance where the printer is defective—courts are likely to apply the relevant provisions of Article 2 to resolve the entire dispute.¹³⁶ However, where a transaction involves the provision of goods and services a court may apply Article 2 only to the goods aspect of the contract and the common law to the services portion of the transaction.¹³⁷

Additionally, using the factors set forth by the Fourth Circuit in *Coakley & Williams, Inc. v. Shatterproof Glass Corp.*,¹³⁸ the nature of the seller's business should also be considered. How should courts assess the nature of Amazon's business? Is the percentage of profits generated by the sale of goods versus services or the number of goods sold directly by Amazon in comparison to the number of goods sold by third party sellers on Amazon determinative? Amazon is in the business of selling various goods but, as more products become enabled with DRS and as more buyers begin to use the Amazon Dash Button, these questions may not be easily answered. Additionally, where the purchase of an IOT device is accompanied by a software license agreement, multiple contracts for services, such as a mobile application or

136. See NAT'L CONSUMER LAW CTR., SALES OF GOODS AND SERVICES 162 (2d ed. 1989) (“[I]f the contract is predominantly for the sale of goods, the UCC is applied to the full transaction.”).

137. See *Stephenson v. Frazier*, 399 N.E.2d 794, 797–98 (Ind. Ct. App. 1980) (applying the common law to the services aspect of a hybrid transaction and the UCC to the goods aspect of the transaction). Courts have reached varying results on this issue with most seemingly rejecting this approach. See *Hirschfield Sons, Co. v. Colt Indus. Operating Corp.*, 309 N.W.2d 714 (Mich. Ct. App. 1981) (relying on the rationale in *Stephenson* and declining to apply Article 2 to a transaction in which there was a separate price for installation and the claim related exclusively to the installation aspect of the contract); *Reynolds v. Preferred Mut. Ins. Co.* (Mass. App. Div. 1972) (applying UCC implied warranties to the sale and installation of gutters in the plaintiff's home and finding the warranties were breached due to the faulty installation); see also *Milau Assocs. v. North Ave. Dev. Corp.*, 42 N.Y.2d 482, 486–87 (N.Y. 1977) (questioning whether the UCC's implied warranties can apply only to the goods aspect of a hybrid transaction and finding that the contract at issue was predominately service oriented); *Paint Prod. Co. v. AA-1 Steel Equip. Co.*, 393 A.2d 1317 (Conn. Super. Ct. 1977) (finding that “a contract for the sale of a product and its installation . . . should be considered as a unified whole and not divided into separate and independent parts.”).

138. 706 F.2d 456 (4th Cir. 1983).

installation services, and a contract explaining the company's terms and conditions for the sale of the device, what is the predominant purpose of such a transaction given that the entire transaction is subject to multiple separate and distinct agreements? Given the deficiencies of the predominant purpose test, the gravamen of the claim test has been offered as an alternative.¹³⁹

2. Gravamen of the Claim Test

The gravamen of the claim test focuses on whether the dispute concerns the goods or the services.¹⁴⁰ If the claim relates to the services, then Article 2 does not apply and, if the dispute relates to the goods aspect of the transaction, then Article 2 will govern.¹⁴¹ When strictly applied, this test may supply some certainty to sellers and buyers. Parties would know in advance that, if the goods aspect of the transaction formed the gravamen of the action for relief, Article 2 would apply and its accompanying warranties would be applicable unless specifically disclaimed.

The gravamen of the claim test has been heavily criticized for several reasons.¹⁴² The test provides very little guidance in

139. See HAWKLAND, *supra* note 8, § 2-102 (discussing the gravamen of the claim test and noting that the test “has not won widespread acceptance in the courts.”).

140. See *id.* § 2-51 (“Under this test, Article 2 would apply to the goods aspect of the transaction if that aspect of the transaction formed the gravamen of the action for relief.”); see also *Anthony Pools v. Sheehan*, 455 A.2d 434, 441 (Md. 1983) (noting that where consumer goods “are sold and monetary loss or personal injury is claimed to have resulted from a defect in the consumer goods,” the provisions of the Maryland U.C.C. dealing with implied warranties apply, “even if the transaction is predominately one for the rendering of consumer services”).

141. See *J.O. Hooker & Sons, Inc. v. Roberts Cabinet Co.*, 683 So. 2d 396, 400 (Miss. 1996) (“[I]n such a mixed transaction, whether or not the contract should be interpreted under the UCC or our general contract law should depend upon the nature of the contract and also upon whether the dispute in question primarily concerns the goods furnished or the services rendered under the contract.”).

142. See, e.g., Austin Bodnar, *Mixed Transactions for Goods and Services: The Need for Consistency in Choosing the Governing Law*, 27 SAINT THOMAS L. REV. 225, 238 (2015) (“[T]he main problem with using the gravamen standard is that

attempting to assess whether the plaintiff's claim relates to the goods or the services.¹⁴³ In order to determine which law governs a transaction, one of the parties must first bring suit and then await the court's determination of whether the dispute is about the goods or the services.¹⁴⁴

The test also presents difficulties when applied to IOT transactions. For example, a plaintiff may be unsatisfied with various IOT services but drafts the complaint to imply that the dispute is about the goods. Where the ordering service software is directly embedded within the goods or the service is provided through the goods, such as when a Brita water pitcher is integrated with Amazon's DRS, how does one apply the gravamen test where the plaintiff wants to contest contract formation? In that instance, is the claim related to the Brita filter, the pitcher, Amazon's DRS, or defective software? The gravamen of the claim test is difficult to apply in such an instance.

Consider a buyer that obtains an IOT device and simultaneously enters into an agreement with the manufacturer for an energy monitoring service. The IOT device collects data monthly about the owner's heating and air conditioning usage and adjusts the temperature in the owner's office. Assume further that after the owner authorizes its utility providers to share data with the IOT manufacturer, the energy reporting service combines data from the IOT device and utility companies (water, gas and electric) to generate a complete picture of the owner's energy use. If a plaintiff believes that this IOT device is ineffectively or incorrectly monitoring and impacting energy use as described in the monthly energy reports, is the defect simply due to the energy reporting service or is the device and the embedded software itself defective, thereby causing the misleading reports? Moreover, if a plaintiff contends that both

it prevents parties from knowing what law governs their contract at its inception, which leaves the parties unaware of their rights and obligations under the contract until a dispute arises.”).

143. See RUSCH & SEPINUCK, *supra* note 120, at 26 (detailing the requirements of the test).

144. See Bodnar, *supra* note 142, at 238 (discussing conflicting parties' uncertainty as to the law governing their dispute prior to a judge's determination).

the IOT services and the device are inadequate or defective, should we view the gravamen of the dispute as concerning the services or the goods? Application of the gravamen of the claim test is unlikely to yield consistent and dispositive answers in the IOT context.

B. Service Contracts and Other Sources of Law

As discussed in Part III above, a court may apply Article 2 and its implied warranties to the goods aspect of the hybrid transaction and a different source of law to the non-goods aspect of the transaction.¹⁴⁵ Thus, courts could use another source of law, such as the common law, to resolve the parties' dispute where a component test is used or where a court determines under the gravamen of the claim or the predominant purpose tests that Article 2 does not apply to a hybrid transaction. Further, the Warranty Act may apply to transactions that are subject to Article 2 and the common law.

1. Common Law Warranties

The implied warranties of merchantability and fitness for a particular purpose which are found in the UCC are likely not applicable to service contracts.¹⁴⁶ To the extent that a court

145. See *Foster v. Colo. Radio Corp.*, 381 F.2d 222, 226 (10th Cir. 1967) (finding that Article 2 can be applied to the goods aspect of a transaction which involved the sale of office equipment and furnishings, real estate, studios and transmission equipment). This test assumes that a hybrid transaction is comprised of two separate transactions—one for goods and one for non-goods, and does not appear to depend mainly on whether the dispute relates to the goods, but rather evaluates whether a portion of the transaction meets the definition of goods. Taylor, *infra* note 146, at 253 (distinguishing the components test from the gravamen of the claim test). To the extent that the component test is used, multiple sources of law including the common law and the UCC may apply to an IOT transaction.

146. See Ellen Taylor, *Applicability of Strict Liability Warranty Theories to Service Transactions*, 47 S.C. L. REV. 231, 255 (1996) (“[T]he majority position is still that implied warranties do not attach to service transactions”); see also *Cargill, Inc. v. Ron Burge Trucking, Inc.*, No. 11-2394, 2013 WL 608520, at *3 (D. Minn. Feb. 19, 2013) (finding that the implied warranty of fitness for a particular

determines that Article 2 does not apply to an IOT transaction after applying the predominant purpose or the gravamen of the claim tests, a consumer is unlikely to receive the benefits of the implied warranties under Article 2. However, a consumer could attempt to use implied warranties that may arise under the common law to fill this gap.

While the manufacturer of an IOT device may provide an express warranty, such a warranty is likely to extend to the device but not to the product replacement, monitoring, and other online services provided in connection with the device. For instance, the manufacturer of a Brother printer may provide a limited express warranty that covers the printer and its accessories, but DRS as well as the embedded firmware provided by Brother are likely not subject to the warranty.¹⁴⁷ Similarly, Nest's terms of use explicitly provide that the company makes no warranties that its "services will be available on an uninterrupted basis, timely, secure or error-free and in no event will its services constitute a warranty."¹⁴⁸

Courts have imposed implied duties on service contracts involving professionals but have been reluctant to extend implied warranties to all service contracts.¹⁴⁹ For instance, in a

purpose did not arise by operation of law in service contracts).

147. See *Amazon Dash Replenishment Terms of Use*, supra note 57; see also *Conditions of Use*, supra note 57; *Amazon's Dash Replenishment Service Brother User Terms*, supra note 56 (noting that Brother provides no warranties with respect to the DRS service or its embedded firmware); *Brother Digital Color One-Year Limited Warranty and Replacement Service*, BROTHER INDUSTRIES (2012), http://www.brother-usa.com/VirData/Content/en-US/Printers/WarrantyDocuments/WarrantyStatements/DigitalColor_1YRExchangeWarranty_06052012.pdf (providing for a limited warranty and replacement service which covers the machine and accompanying consumable and accessory items).

148. See *Limited Warranty Thermostat*, supra note 79 (noting that all product information and services provided by Nest are provided on an "as-is" basis); see also *Terms of Service*, NEST supra note 76 (noting that all warranties for the services provided by Nest, including my energy service, are disclaimed).

149. See, e.g., *Pearl Invs. LLC v. Std. I/O, Inc.*, 257 F. Supp. 2d 326, 352 (2003) (noting that courts have been wary of recognizing implied warranties in the context of performance of services, doing so only for compelling public-policy reasons); *Bloomsburg Mills, Inc. v. Sardoni Constr. Co.*, 164 A.2d 201, 203 (Pa. 1960) (noting that "while an architect is not an absolute insurer of perfect plans, he is called upon to prepare plans and specifications which will give the structure so designed reasonable fitness for its intended use, and he impliedly warrants

2016 decision, a Michigan court found that the implied warranty of fitness for a particular purpose did not apply to a contract for the provision of architectural services.¹⁵⁰ Despite this majority position, courts have imposed implied warranties in service contracts in some cases, such as the implied warranty of workmanlike or skillful performance and the implied warranty of fitness, habitability, and suitability.¹⁵¹ Other courts have held that implied warranties are not applicable where service contracts are at issue as they are akin to the duty of care in a negligence action and as such cannot give rise to a breach of warranty claim.¹⁵²

their sufficiency for that purpose”); *E. Grand Forks v. Steele*, 141 N.W. 181, 182 (Minn. 1913) (noting that “[d]efendants represented themselves as expert accountants, which implied that they were skilled in that class of work. In accepting employment as expert accountants, they undertook, and the plaintiff had the right to expect, that in the performance of their duties they would exercise the average ability and skill of those engaged in that branch of skilled labor”). *But see* *Audlane Lumber & Builders Supply, Inc. v. D. E. Britt Assocs., Inc.*, 168 So. 2d 333, 335 (Fla. Dist. Ct. App. 1964) (finding that an engineer does not warrant his services to be merchantability or fit for an intended use but rather warrants that he will exercise his skill pursuant to a reasonable standard of care and breach of this warranty occurs where the professional is negligent).

150. *See* *Albion College v. Stockade Buildings, Inc.*, No. 322917, 2016 Mich. App. LEXIS 998, at *6 (Mich. Ct. App. May 17, 2016) (holding that the implied warranty of fitness for a particular purposes applies only to the sale of goods or electricity).

151. *See* *Air Heaters, Inc. v. Johnson Elec., Inc.*, 258 N.W.2d 649, 653 (N.D. 1977) (noting that an implied warranty of fitness may apply to construction contracts); *Omaha Pollution Control Corp. v. Carver-Greenfield Corp.*, 413 F. Supp. 1069, 1085–86 (D. Neb. 1976) (holding that an implied warranty of merchantability and fitness attached to the design and construction of a sewage plant); *Corral v. Rollins Protective Servs. Co.*, 732 P.2d 1260, 1268 (Kan. 1987) (reasoning that warranties, express or implied, may be present in any type of contract including sales, leases, bailments, and service agreements, and holding that the trial court was in error when it concluded that there could be no implied warranties outside the ambit of the UCC); *Weeks v. Slavik Builders, Inc.*, 180 N.W.2d 503, 506–07 (Mich. Ct. App. 1970) (extending the implied warranty of fitness to the sale of new residential houses); *Hoye v. Century Builders, Inc.*, 329 P.2d 474, 476 (Wash. 1958) (holding that the implied warranty of habitability applied to a home construction contract). *See generally* E. Allan Farnsworth, *Implied Warranties of Quality in Non-Sales Cases*, 57 COLUM. L. REV. 653 (1957) (identifying and exploring various implied warranties).

152. *See* *Cargill, Inc. v. Ron Burge Trucking, Inc.*, No. 11-2394, 2013 WL 608520, at *3 (D. Minn. Feb. 19, 2013) (noting that in a service contract any implied duty to perform the work or services skillfully, carefully, and in a

As discussed above, IOT transactions will typically involve the provision of ongoing services by retailers such as Amazon and Nest.¹⁵³ However, as currently envisioned, IOT service contracts between consumers and businesses do not involve the construction of a device but rather involve the use of pre-existing ordering or application services. Thus, the applicability of these types of common-law warranties to consumer IOT transactions is questionable. In contrast, in the industrial IOT setting, businesses may require sellers to design, construct and customize IOT devices for use in manufacturing and business operations. One could posit that common-law implied warranties should be extended to cover services in such contracts or, alternatively, that courts should apply the UCC's implied warranties by analogy.¹⁵⁴ Given the fact that most courts are reluctant to extend such warranties to service contracts it is unlikely that this argument will succeed.

Where an IOT hybrid transaction involves the installation or provision of a device which impacts the habitability of a home, one could argue that the implied warranties found by courts to be applicable to service contracts should be extended to such IOT hybrid transactions. However, the implied warranty of habitability has historically applied to the sale or construction of a new home or in the tenancy context, and not to the performance of goods or services within the home after construction.¹⁵⁵

workmanlike manner is a duty of care and not a warranty that can give rise to a breach of warranty claim); *see also* Pepsi Cola Bottling Co. v. Superior Burner Serv. Co., 427 P.2d 833, 841–42 (Alaska 1967) (finding that a cause of action for breach of an implied warranty to repair in a workmanlike manner is identical to a negligence claim).

153. *See supra* Part I (discussing and providing examples of retailers providing ongoing services in IOT transactions).

154. *See generally* Peter A. Alces & Aaron S. Book, *When Y2K Causes "Economic Loss" to "Other Property,"* 84 MINN. L. REV. 1 (1999) (contending that, where a court determines that the same commercial principles are implicated in a non-Article 2 contract as are vindicated by the warranty provisions of Articles 2 and 2A, it would be entirely appropriate for the court to apply the UCC implied warranty provisions by analogy).

155. *See* Miller v. Cannon Hill Estates, Ltd., 2 K.B. 113, 121 (1931) ("It is plain that in those circumstances there is an implication of law that the house shall be reasonably fit for the purpose for which it is required, that is for human

IOT contracts contain warranty disclaimers and limitation of damages provisions.¹⁵⁶ To the extent that a consumer is physically injured by an IOT device, Article 2 provides that a limitation of consequential damages for personal injury in the case of consumer goods is viewed as prima facie unconscionable.¹⁵⁷ However, while not absolute, this additional protection for consumers is likely only available where Article 2 applies to the transaction unless another relevant source of law contains a similar provision. Courts are also reluctant to strike down contract terms on the grounds of unconscionability.¹⁵⁸

Additionally, pursuant to section 1-103 of the UCC, common-law warranties in sale of goods transactions may be displaced by Article 2's implied warranties.¹⁵⁹ Courts have held that implied warranties are applicable to goods not services. For instance, in *Dobisky v. Rand*,¹⁶⁰ the court stated “[New York] does not recognize a cause of action in breach of warranty for the performance of services.”¹⁶¹ Similarly, in *Aegis Productions, Inc. v. Arriflex Corp. of America*,¹⁶² the court stated “warranties are

dwelling.”); see also *Lane v. Trenholm Bldg. Co.*, 229 S.E.2d 728, 730–31 (S.C. 1976) (holding that the implied warranty of habitability is applicable even where the seller of the new home is not the builder); *Rutledge v. Dodenhoff*, 175 S.E.2d 792, 795 (S.C. 1970) (holding that an implied warranty of habitability applies to a contract involving the construction of a new home).

156. See generally, e.g., *Amazon Dash Button Terms of Use, supra* note 57; *Conditions of Use, supra* note 57.

157. See U.C.C. § 2-719(3) (AM. LAW INST. & UNIF. LAW COMM'N 2002) (“Consequential damages may be limited or excluded unless the limitation or exclusion is unconscionable. Limitation of consequential damages for injury to the person in the case of consumer goods is prima facie unconscionable but limitation of damages where the loss is commercial is not.”).

158. See, e.g., *In re Emery-Watson*, 412 B.R. 670, 674 (Bankr. D. Del. 2009) (“[C]ourts generally, and this Court in particular, are reluctant to void contracts on grounds of unconscionability . . .”).

159. See U.C.C. § 1-103(b) (AM. LAW INST. & UNIF. LAW COMM'N 2002) (“Unless displaced by particular provisions of the Uniform Commercial Code, the principles of law and equity, including the law merchant and the law relative to capacity to contract, principal and agent, estoppel, fraud, misrepresentation, duress, coercion, mistake, bankruptcy, and other validating or invalidating cause supplement its provisions.”).

160. 670 N.Y.S.2d 606 (N.Y. App. Div. 1998).

161. *Id.* at 608.

162. *Aegis Prods., Inc. v. Arriflex Corp. of Am.*, 268 N.Y.S.2d 185, 187 (N.Y.

limited to [the] sales of goods. No warranty attaches to the performance of a service. . . . No such right has ever been extended to include the consequence of a performance of a service.”¹⁶³ Thus, it is questionable whether common-law implied warranties will be applicable to IOT transactions.

Additionally, even if one were to contend that common-law implied warranties are applicable to a transaction, such an argument may fail where there is an express agreement between the parties. A party may be able to successfully defend against such claims by contending that the common law disfavors implied contract terms and that the parties have an express agreement disclaiming such warranties.¹⁶⁴

2. Warranty Act

In addition to state statutes and common law rules regarding implied warranties, the Warranty Act may also be applicable to consumer IOT transactions and afford additional protections to consumers.¹⁶⁵ The Warranty Act applies to written warranties of consumer products, implied warranties that arise under state law, and service contracts relating to consumer products.¹⁶⁶ IOT devices may meet the definition of consumer products under the Warranty Act as these devices are tangible personal property distributed in commerce and they

App. Div. 1966).

163. *Id.* at 187.

164. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 980 (S.D. Cal. 2014) (holding that plaintiff’s common law implied warranty claims failed because the terms of the parties’ agreement contained a disclaimer of warranties and statutory and common law implied warranties can be disclaimed by conspicuous language in a contract presented to the consumer at the time of the transaction).

165. Magnuson-Moss Warranty–Federal Trade Commission Improvement Act, Pub. L. No. 93-637, § 108(A), 88 Stat. 2183 (1975) (codified at 15 U.S.C. §§ 2301–2312 (2006)).

166. *See RUSCH & SEPINUCK, supra* note 120, at 337 (stating that “the Magnuson-Moss Act . . . does not have a single provision that identifies the situations to which it applies. Therefore, one must peruse the operative sections of the act, identify key words, and then review the statutory definitions of those terms to ascertain the scope of the act”).

can be used for personal, family, or household purposes.¹⁶⁷ However, it is unclear whether the definition of tangible personal property and, therefore, consumer products under the statute would include the transfer of software.¹⁶⁸

The statute provides a consumer with a cause of action where a consumer suffers harm from a supplier's, warrantor's or service contractor's violation of the provisions of the Warranty Act, or the breach of a written warranty, implied warranty or service contract.¹⁶⁹ The Warranty Act does not require that suppliers provide a warranty, but instead, mandates that where a warrantor provides a written warranty, the warrantor must comply with adopted Federal Trade Commission (FTC) rules.¹⁷⁰

To the extent that the Warranty Act covers IOT hybrid transactions, it would prohibit a supplier from disclaiming an implied warranty when a written warranty is provided for an IOT device or if "at the time of sale, or within 90 days thereafter, [the] supplier enters into a service contract with the consumer which applies to [the] consumer product."¹⁷¹ Under the

167. *See id.* § 2301(1) (defining consumer products as tangible personal property which is normally used for personal, family, or household purposes).

168. *See* 2 BARKLEY CLARK & CHRISTOPHER SMITH, THE LAW OF PRODUCT WARRANTIES § 14:3 (2015) (noting that, as of 2015, the Federal Trade Commission has not elaborated on this issue). *But see generally* Microsoft Corp. v. Manning, 914 S.W.2d 602 (Tex. App. 1995) (suggesting that the Warranty Act can apply to the transfer of software programs and information products).

169. *See* 15 U.S.C. § 2310(d) (2012) (providing and detailing remedial procedures under the Warranty Act); *see also* RUSCH & SEPINUCK, *supra* note 120, at 336 (contending that the key benefit of the Warranty Act "is that if a warrantor violates its obligations under the Act, the injured 'consumer' is entitled to recover the reasonable attorney's fees incurred in any successful enforcement action . . . [and] [t]his right is critical because it gives injured consumers the ability to prosecute a claim that would otherwise be too small to justify the expense involved.").

170. *See* 15 U.S.C. § 2302(b) (providing for various requirements which attach upon provision of a written warranty and adoption of the FTC rules).

171. *Id.* § 2308(a). Under the statute an implied warranty is defined as an implied warranty that arises under state law (as modified by the act's provisions on implied warranties and minimum standards for warranties) in connection with the sale of a consumer product. *Id.* § 2301(7). A written warranty is defined as a written affirmation of fact or written promise made in connection with the sale of a consumer product by a supplier to a buyer which relates to the nature of the material or workmanship and affirms or promises that such material or workmanship is defect free or will meet a specified level of performance over a

Warranty Act, implied warranties are defined as those which “arise under state law” and therefore, the Warranty Act’s prohibition of implied warranty disclaimers may only apply to the extent that the implied warranties “arise under state law.” If a court were to determine that Article 2 does not apply to a transaction, the implied warranties of merchantability and fitness for a particular purpose would not “arise under state law” for purposes of the Warranty Act. On the other hand, one could contend that the definition of an implied warranty under the Warranty Act suggests that it is modified by the provisions of the act prohibiting implied warranty disclaimers and these provisions apply to any implied warranty, including implied warranties that may arise under the common law. However, as noted in Part III(b)(1) above, some courts have found that implied warranties are primarily applicable to goods, which are usually governed by Article 2 (or 2A of the UCC which has similar implied warranties), and given the provisions of the Warranty Act that refer to a sale, unless another source of law requires otherwise, these courts may be unwilling to apply to IOT transactions implied warranties that do not arise under the UCC.¹⁷² Thus, in order for the Warranty Act’s prohibition on the disclaimer of implied warranties to be effective at protecting consumers, it is likely that Article 2 must apply to the transaction.

A supplier that offers a limited warranty rather than a full warranty is free to limit the duration of the implied warranties to the duration of “a written warranty of reasonable duration.”¹⁷³ Where the manufacturer provides a written warranty that lasts for several years, this may be beneficial to consumers. However, that may not be the case where the duration of the written warranty is short.

specified period of time, or any undertaking in writing in connection with the sale by a supplier of a consumer product to refund, repair, replace, or take other remedial action with respect to such product in the event that such product fails to meet the specifications set forth in the undertaking, which becomes part of the basis of the bargain. *Id.* § 2301(6).

172. See generally Part III.

173. See Magnuson-Moss Warranty Act § 108(b) (2012) (stating that such a duration limitation must be conspicuous and conscionable).

Recent studies of warranties subject to the Warranty Act have found that manufacturers are routinely providing consumers with limited rather than full warranties.¹⁷⁴ Nest labels the warranty it provides for its IOT products as a “limited warranty” and the company also attempts to limit the duration of any applicable implied warranties to the duration of the written warranty.¹⁷⁵ To the extent that IOT manufacturers provide limited rather than full warranties, consumers may not receive the additional protections provided under the Warranty Act. Where a full warranty is provided, a supplier may not limit the duration of implied warranties or “impose any unreasonable duty as a condition of warranty coverage.”¹⁷⁶

Today, warranties are seven times lengthier than they were in 1977 (two years after the Warranty Act was enacted).¹⁷⁷ As a result, consumers may be less likely to read such warranties.¹⁷⁸ This is particularly concerning given the fact that the Warranty Act was intended to facilitate consumer understanding of warranties and to allow consumers to easily differentiate between reliable and non-reliable products. According to a 2012 warranty analysis, manufacturers also routinely ignore the Warranty Act’s prohibition of implied warranty disclaimers and include disclaimer language in their terms and conditions.¹⁷⁹ The FTC has been criticized for a perceived failure to effectively implement the statute.¹⁸⁰ Increased FTC enforcement of the Warranty Act is needed. Both Nest and Amazon’s terms of service contain disclaimers of the implied Article 2

174. See Janet W. Steverson & Aaron Munter, *Then and Now: Reviving the Promise of the Magnuson-Moss Warranty Act*, 63 KAN. L. REV. 227, 245 (2015) (surveying recent warranties).

175. *Limited Warranty Smoke Alarm*, NEST, <https://nest.com/legal/warranty/smokealarm/> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

176. Steverson & Munter, *supra* note 174, at 244. See generally Magnuson-Moss Warranty Act § 2304(b)(1).

177. Steverson & Munter, *supra* note 174, at 245–53.

178. See *id.* (outlining the growth in the length of warranties).

179. *Id.* at 254.

180. See *id.* at 256 (charging the FTC with failing to actively pursue violators).

warranties.¹⁸¹ The inclusion of such disclaimer language may discourage consumers from bringing suit even where the disclaimer is invalid under the Warranty Act or state law.

The Warranty Act also permits suppliers to enter into service contracts with consumers in lieu of a warranty provided that contract terms are conspicuously disclosed and easily understandable.¹⁸² The service contracts covered by the Warranty Act are those in which a seller has made a commitment to maintain or repair consumer products over a specified period.¹⁸³ As discussed in Part II above, IOT service contracts are distinct from the maintenance service contracts typically provided by service providers. Of course, companies manufacturing IOT devices may ultimately offer standard service contracts for the maintenance of IOT devices, thereby potentially making the Warranty Act applicable to the transaction.

IOT companies such as Nest currently do not provide warranties for the services provided in connection with an IOT device, but a limited warranty applies to its devices including Dropcam, the Nest Learning Thermostat, Nest Protect and Nest Cam.¹⁸⁴ Because the services provided in connection with IOT devices may not qualify as a service contract under the Warranty Act, the Warranty Act's prohibition on the disclaimer of implied warranties may not apply to the majority of services currently provided by IOT companies where a written warranty is not provided.

Despite the consumer protections contained in the Warranty Act, some courts have unfortunately limited the effectiveness of the statute.¹⁸⁵ Some courts have held that where

181. *Limited Warranty Smoke Alarm*, *supra* note 175.

182. *See* 15 U.S.C. § 2306 (2012) (addressing service contracts on consumer products).

183. *See id.* § 2301(8) (defining a service contract as “a contract in writing to perform, over a fixed period of time or for a specified duration, services relating to the maintenance or repair (or both) of a consumer product”).

184. *Terms of Service*, *supra* note 76; *see also Limited Warranty Thermostat*, *supra* note 79 (providing for a two-year limited warranty for the Nest thermostat); *End User License Agreement*, *supra* note 78 (noting that the software is sold “as is” and all implied warranties are disclaimed).

185. *See* Janet W. Steverson, *The Unfulfilled Promise of the Magnuson Moss*

a supplier has not provided a written warranty, consumers are barred from bringing an action for breach of implied warranties and they have imposed privity requirements in warranty claims.¹⁸⁶ In some jurisdictions, vertical privity is still a requirement for breach of implied warranty claims and as a result, courts have required that consumers satisfy state law privity requirements in order to bring a breach of warranty claim under the Warranty Act.¹⁸⁷ These courts have ignored the provisions of the Warranty Act, which describe the parties who may be sued and those that are authorized to bring suit under the statute.¹⁸⁸ Under the statute, both a seller or manufacturer may qualify as a warrantor and any consumer to whom the goods are transferred is entitled to sue.¹⁸⁹ These provisions suggest

Warranty Act, 18 LEWIS & CLARK L. REV. 155, 176–77 (2014) (noting that courts have not allowed consumers to bring bare implied breach of warranty claims nor held that the act overturns common law privity requirements).

186. See *Kutzler v. Thor Indus., Inc.*, No. 03 C 2389, 2003 WL 21654260, at *7 (N.D. Ill. July 14, 2003) (finding that privity is required to assert an implied warranty claim in an economic loss case and reasoning that revocation of acceptance under § 2310(d) of the Warranty Act is unavailable against a manufacturer who is not a party to the sales because § 2-608 of the UCC on its face contemplates that the remedy of revocation is available only against a seller); *Hamdan v. Land Rover North Am., Inc.*, No. 03 C 2051, 2003 WL 21911244, at *2 (N.D. Ill. Aug. 8, 2003) (concluding that a plaintiff is barred from pursuing an implied warranty claim under Magnuson-Moss if state law requires privity for the claim to succeed); *McNamara v. Nomeco Bldg. Specialties, Inc.*, 26 F. Supp. 2d 1168, 1175 (D. Minn. 1998) (concluding that there was no Magnuson Act claim for breach of implied warranty since there was no written warranty). *But see* *Mattuck v. DaimlerChrysler Corp.*, 852 N.E.2d 485, 496 (Ill. App. Ct. 2006), *vacated by* 877 N.E.2d 1, 1 (Ill. 2007) (finding that the Warranty Act relaxes the privity requirement found under the UCC); *Ventura v. Ford Motor Corp.*, 433 A.2d 801, 808 (N.J. Super. Ct. App. Div. 1981) (finding that the Warranty Act eliminates privity requirements).

187. See *Curl v. Volkswagen of Am., Inc.*, 871 N.E.2d 1141, 1145–47 (Ohio 2007) (“Ohio continues to require privity as to contract claims.”); *Cerasani v. Am. Honda Motor Co.*, 916 So. 2d 843, 847 (Fla. Dist. Ct. App. 2005) (concluding that the Magnuson-Moss Act applied to the transaction but the act does not supersede privity requirements for implied warranties); *Flory v. Silvercrest Indus., Inc.*, 633 P.2d 383, 386–87 (Ariz. 1981) (imposing a privity requirement on implied warranty claims).

188. See *Steverson*, *supra* note 185, at 178 (cataloging the causes of action explicitly authorized the MMWA).

189. Magnuson-Moss Warranty Act § 101(3), (4) & (5) (2012).

that vertical privity is not a requirement for suit.¹⁹⁰ Thus, while the Warranty Act may be applicable to some IOT transactions the effectiveness of the Warranty Act in providing adequate protection to consumers is questionable.

C. Software and Goods Under Article 2

As noted in Part II above, hybrid IOT transactions involve not only the provision of services but also software. Thus, UCC case law on software transactions is germane to any discussion of Article 2's role in determinations evaluating hybrid IOT transactions. Hybrid software transactions frequently arise where software is provided along with hardware or other products.¹⁹¹ In the consumer context, a hybrid transaction may also arise where software, which may be viewed as a good, is provided along with services, such as installation, debugging, and other support services.¹⁹²

190. See *id.* § 2310(d)(1) (listing and authorizing cognizable claims); Steverson, *supra* note 185, at 186 (arguing that by authorizing suits against warrantors, suppliers, and service contractors, § 2310(d)(1) does away with any requirement of vertical privity); see also CAROLYN L. CARTER ET AL., NAT'L CONSUMER LAW CTR., CONSUMER WARRANTY LAW: LEMON LAW, MAGNUSON-MOSS, UCC, MANUFACTURED HOME, AND OTHER WARRANTY STATUTES § 2.3.6.2 (4th ed. 2010) (“[T]he Act’s definitions of supplier and warrantor indicate that vertical privity is not required. The definition of supplier includes those who make products directly or indirectly available to consumers, encompassing remote manufacturers who indirectly make products available to consumers.”).

191. See *RRX Indus., Inc. v. Lab-Con, Inc.*, 772 F.2d 543, 546 (9th Cir. 1985) (finding that the sales aspect of a software transaction for the transfer of prepackaged software predominated and the other aspects of the transfer were incidental to the sale of the software package and thus the transaction was a sale of goods subject to Article 2); *Triangle Underwriters, Inc. v. Honeywell, Inc.* 604 F.2d 737, 742–43 (2d Cir. 1979) (evaluating custom application software specifically designed for individual needs of the customer and finding that the predominant factor was the sale of goods while services were merely incidental); *Chatlos Sys., Inc. v. Nat'l Cash Register Corp.*, 479 F. Supp. 738, 742 (D. N.J. 1979) (finding that a contract for the provision of hardware and software was a sale of goods notwithstanding the incidental service aspects of the transaction).

192. See Andrew Rodau, *Computer Software: Does Article 2 of the Uniform Commercial Code Apply?*, 35 EMORY L.J. 853, 914–16 (1986) (describing typical transactions in which the provision of software is accompanied by an offering of ancillary services).

In some instances, courts have applied Article 2 to transactions involving software.¹⁹³ For instance, in *Micro Data Base Systems v. Dharma Systems*,¹⁹⁴ the Seventh Circuit stated “we can think of no reason why the UCC is not suitable to govern disputes arising from the sale of custom software—so we’ll follow it.”¹⁹⁵ Courts have also found that an agreement for the transfer of “off-the-rack” software is a transaction in goods.¹⁹⁶

In contrast, some courts have reasoned that Article 2 applies only to sales rather than to licenses.¹⁹⁷ The “sale vs.

193. See *Advent Sys., Ltd. v. Unisys Corp.*, 925 F.2d 670, 675 (3d Cir. 1991) (noting that intellectual property law does not prevent the application of Article 2 and that “[t]he fact that some [software] programs may be tailored for specific purposes need not alter their status as ‘goods’”). See generally *Dreier Co., Inc. v. Unitronix Corp.* 527 A.2d 875 (N.J. Super. App. Div. 1986) (applying Article 2 to a transaction involving the sale of a computer system including hardware and payroll software). Scholars have also argued for the application of Article 2 to transactions involving the provision of software products. See Jean Braucher, *supra* note 34, at 241 (contending that one body of law should govern transactions involving hardware and software); Bonna Lynn Horovitz, Note, *Computer Software as a Good Under the Uniform Commercial Code: Taking a Byte Out of the Intangibility Myth*, 65 B.U. L. REV. 129, 136 (1985) (contending that all software transactions which are not clearly and exclusively contracts for the provision of services should be subject to Article 2’s provisions, regardless of software’s inherent intangibility, regardless of its labor-intensive element, and regardless of its tendency to be conveyed in forms other than a traditional sale).

194. 148 F.3d 649 (7th Cir. 1998).

195. See *id.* at 654 (noting that Article 2 can apply to custom software licenses).

196. See *Gross v. Symantec Corp.*, No. C 12–00154 CRB (N.D. Cal. July 31, 2012) (reasoning that downloaded software was a good subject to the UCC similar to a sale software in a store and did not include installation, training, maintenance, or upgrading services); *Olcott Int’l & Co. v. Micro Data Base Sys., Inc.*, 793 N.E. 2d 1063, 1071 (Ind. Ct. App. 2003) (concluding that Article 2 of UCC applied to a contract for the purchase of “pre-existing, standardized” software); *SoftMan Prods. Co. v. Adobe Sys., Inc.*, 171 F. Supp. 2d 1075, 1084 (C.D. Cal. 2001) (reasoning that a transaction related to Adobe software was a sale of goods and not a license because the purchaser obtains a single copy of the software, for a single price, which constitutes the entire payment for the ‘license,’ which runs for an indefinite term without renewal provisions).

197. See generally *Digital Ally, Inc. v. Z3 Tech., LLC*, Case No. 09-2292-KGS, 2010 U.S. Dist. LEXIS 103715, at *32 (D. Kan. Sept. 30, 2010) (finding that Article 2 does not apply to a software licensing agreement as title to the product was not transferred to the buyer); *Adobe Sys. Inc. v. One Stop Micro*, 84 F. Supp. 2d 1086 (N.D. Cal. 2000) (declining to apply Article 2 to prepackaged software products such as Adobe Photoshop); *Kane v. Fed. Express Corp.*, No. CV-990078971S, 2001 Conn. Super. LEXIS 2536 (Conn. Super. Aug. 28, 2001) (noting

license” distinction is an important one. Where a court finds that a transaction is a license of software rather than a sale, the terms of the licensing agreement will normally control the transaction subject to applicable contract formation rules and defenses to enforcement.¹⁹⁸ If the software transaction is a sale and is subject to Article 2, several additional issues arise. First, Article 2 frequently allows parties to contract out of provisions that may be beneficial to buyers. The ability of parties to disclaim implied warranties is one such area. Second, state consumer statutes, as well as a state’s version of the UCC, may in some instances provide additional protection to consumers. For instance, some jurisdictions prohibit the disclaimer of implied warranties in consumer transactions.¹⁹⁹ State unfair and deceptive practices statutes may be limited to tangible goods or services. It is questionable whether software constitutes a good under such statutes, as it may not be viewed as tangible even though it may be moveable for purposes of Article 2.²⁰⁰ Of course, software may in some instances qualify

that a transaction cannot be characterized as a sale under Article 2 of the UCC “where it does not contemplate the passage of title from the plaintiff to the defendant”).

198. See Nancy S. Kim, *The Software Licensing Dilemma*, 2008 BYU L. REV. 1103, 1135–36 (2008) [hereinafter Kim, *The Software Licensing Dilemma*] (describing the operation of contract principles once an agreement is determined to be a license).

199. ALA. CODE §§ 7-2-316(5), 7-2-719(4) (1984); CONN. GEN. STAT. ANN. § 42A-2-316 (West 1990); D.C. CODE ANN. § 28:2-316.1 (West 1991); KAN. STAT. ANN. § 50-639(A) (1983); ME. REV. STAT. ANN. tit. 11, § 2-316(5) (1992); MD. CODE ANN. COM. LAW § 2-316.1; MASS. GEN. LAWS ANN. ch. 106, § 2-316.A (1992); MISS. CODE ANN. § 11-7-18; VT. STAT. ANN. tit. 9A, § 2-316(5) (West 1992); W. VA. CODE § 46A-6-107 (1992).

200. See CAL. CIV. CODE § 1761–1770 (West) (defining goods as tangible chattel and services as work, labor, and services for other than a commercial or business use, including services furnished in connection with the sale or repair of goods and prohibiting unfair methods of competition and unfair or deceptive acts or practices in the sale or lease of goods or services to any consumer); see also *Ladore v. Sony Comput. Entm’t Am., LLC*, 75 F. Supp. 3d 1065 (N.D. Cal. 2014) (finding that a video game was a “good” under the California Legal Remedies Act where the software was purchased in a physical medium, as opposed to downloaded from the internet); *Ferrington v. McAfee, Inc.*, 2010 WL 3910169, at *14 (N.D. Cal. Oct. 5, 2010) (holding that California’s Consumer Legal Remedies Act does not cover transactions related to the sale or lease of software as software is not a tangible good or a service for purposes of the Consumer Legal Remedies

as a service, thereby bringing the transaction within the scope of state consumer protection statutes.²⁰¹ Where a software transaction constitutes a sale that is subject to Article 2 rather than a license, the “written document states the licensor’s obligations, but it does not necessarily serve as an effective limitation of those obligations unless those limitations conform to applicable law.”²⁰² Buyers may be more adequately protected where a hybrid transaction is viewed as a sale subject to Article 2 rather than a license.

The application of Article 2 to transactions involving software has been heavily criticized.²⁰³ Article 2 defines a sale as the passing of title from seller to buyer for a price.²⁰⁴ In a software transaction, title to the software may not pass from the seller to the buyer and software may not always satisfy Article 2’s definition of goods—a movable thing.²⁰⁵ However, as

Act, which covers tangible chattel only); OR. REV. STAT. § 646.605(8) (2013) (defining “trade” and “commerce” as “advertising, offering or distributing, whether by sale, rental or otherwise, any real estate, goods or services”); W. VA. CODE § 46A-6-107 (1992) (prohibiting unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce and defining trade or commerce as the advertising, offering for sale, sale or distribution of any goods or services and shall include any trade or commerce, directly or indirectly, affecting the people of the state).

201. See OR. REV. STAT. § 646.605(8) (2013) (defining “trade” and “commerce” as “advertising, offering or distributing, whether by sale, rental or otherwise, any real estate, goods or services”); W. VA. CODE § 46A-6-107 (1992) (disallowing modification of express and implied warranties for goods and for goods alone).

202. Kim, *The Software Licensing Dilemma*, *supra* note 198, at 1139.

203. See generally Lorin Brenan, *Financing Intellectual Property Under Revised Article 9: National and International Conflicts*, 23 HASTINGS COMM. & ENT. L.J. 313, 464 (2001). Scholars have also critiqued the application of implied warranties to computer programs. See generally Joel Wolfson, *Express Warranties and Published Information Content Under Article 2B: Does the Shoe Fit?*, 16 J. MARSHALL J. COMPUTER & INFO. L. 337 (1997); Joel Wolfson, *Electronic Mass Information Providers and Section 552 of the Restatement (Second) of Torts: The First Amendment Casts a Long Shadow*, 29 RUTGERS L. REV. 67 (1997); Jean Braucher, *Why UCITA, Like Article 2B, Is Premature and Unsound*, in A GUIDE TO THE PROPOSED UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (Carol Kunze ed., 1996).

204. U.C.C. § 2-106 (AM. LAW INST. & UNIF. LAW COMM’N 2002).

205. *Id.* § 2-105; see also SAS Inst., Inc. v. World Programming Ltd., 2016 WL 3435196, at *10 (E.D.N.C. June 17, 2016) (finding that a software license agreement did not transfer title and therefore Article 2 did not apply); Ferrington v. McAfee, Inc., 2010 WL 3910169, at *14 (N.D. Cal. Oct. 5, 2010) (concluding that

Professor Jean Braucher notes, the official comments of Article 2 suggest a flexible approach to the concept of title.²⁰⁶ Article 2's provisions do not automatically remove a transaction from its scope simply because a seller attempts to retain title to the goods in the transaction.²⁰⁷ Additionally, software can be viewed as movable as it can be transported through various means, such as on a disc, device, or downloading. Article 2 applies to transactions in goods. The use of the term "transaction" rather than "sale" suggests that Article 2's scope is not limited to agreements in which title is transferred from seller to buyer.²⁰⁸

As Professor Nancy Kim notes, the sale of a software product does not exclude a license of the software and vice versa.²⁰⁹ The sale of an IOT device potentially includes both a purchase by the buyer of the hardware of the IOT device as well as a license to use the accompanying software programs subject to certain restrictions. Article 9 of the UCC recognizes that goods can be sold to a buyer while the purchaser simultaneously receives the right to use the software accompanying the goods

California law did not support the contention that software is a tangible good or a service for purpose of the Consumer Legal Remedies Act, which covers tangible chattels, because software is not tangible); *Berthold Types Ltd. v. Adobe Sys., Inc.*, 101 F. Supp. 2d 697, 698 (N.D. Ill. 2000) ("[T]he UCC does not apply to this transaction because it involves only granting a license and not a sale of goods . . . [A] pure license agreement . . . does not involve transfer of title, and so is not a sale for Article 2 purposes.").

206. See Braucher, *supra* note 34, at 276 (arguing that Article 2 does not use "title" in a formal, non-functional way).

207. See U.C.C. § 2-401 cmt. 1 (AM. LAW INST. & UNIF. LAW COMM'N 2002) (noting that the Article deals with issues between seller and buyer in terms of step by step performance or non-performance under the contract for sale and not in terms of whether or no title to the goods has passed); *id.* § 2-401 (limiting the effect of an attempted reservation of title to a security interest).

208. See *Architectronics, Inc. v. Control Sys.*, 935 F. Supp. 425, 432 (S.D.N.Y. 1996) (noting that "the applicability of Article Two to a transaction is not defeated by the use of a license in lieu of a sale if the license provides for transfer of some of the incidents of goods ownership" (citations omitted)).

209. See Kim, *The Software Licensing Dilemma*, *supra* note 198, at 1140 (contending that the license grant in a software sale transaction is a promise by the licensor that it will not sue as long as the licensee adheres to the stated restrictions).

and the inclusion of such a right does not remove the transaction from the definition of a good under Article 9.²¹⁰

In connection with the purchase of a Nest device, Nest's EULA grants the licensee permission to execute one copy of the device software for personal use for as long as the buyer owns the product.²¹¹ Nest expressly retains all intellectual property rights in the software and the buyer is prohibited from selling, assigning, distributing, copying or reverse engineering the software.²¹² Nest's EULA also provides that certain aspects of the product software may also be subject to open source software licenses.²¹³ Despite this seeming complexity or dominance of software in an IOT transaction, the inclusion of a software license in connection with the sale of a device should not automatically remove the transaction from the scope of Article 2 as restrictions under an EULA, such as Nest's, could still be enforced even if the transaction is subject to Article 2.

Additionally, "whether a particular transaction involving computer software constitutes a 'transaction in goods' depends on various considerations."²¹⁴ In making such a determination, courts often rely on the predominant purpose test.²¹⁵ The application of the predominant purpose test is problematic in the software context as it may also lead to varying results.²¹⁶

In *Architectronics, Inc. v. Control Systems*,²¹⁷ a case involving a software development and license agreement, the court reasoned that the predominant purpose of the transaction was the transfer of intellectual property rights, and therefore

210. U.C.C. § 9-102(44) (AM. LAW INST. & UNIF. LAW COMM'N 2002).

211. *End User License Agreement*, NEST, *supra* note 78.

212. *See id.* (stating that all copyrights, trade secrets, and other intellectual property rights are exclusively the property of NEST and its licensors).

213. *See id.* (harmonizing the open source EULAs with its own).

214. *Dealer Mgmt. Sys. v. Design Auto. Grp., Inc.*, 822 N.E.2d 556, 560 (2005).

215. *See id.* (noting the disagreement in this area, especially on the issue of Article 2's applicability to a transaction that involves software designed for a specific purpose or to suit the needs of a specific buyer).

216. DOUGLAS J. WHALEY & STEPHEN M. MCJOHN, *PROBLEMS AND MATERIALS ON COMMERCIAL LAW* 32 (11th ed. 2016).

217. 935 F. Supp. 425 (S.D.N.Y. 1996).

Article 2 did not apply.²¹⁸ In *TK Power v. Textron*,²¹⁹ the court found that, although the contract called for the provision of mechanical items and prototypes, most of the price paid under the contract was for the developer's "knowledge, skill, and ability" to develop software code and test prototypes, and therefore the contract was for services rather than goods.²²⁰ In *Audio Visual Industry v. Tanzer*,²²¹ the court reasoned that Article 2 applied to a transaction involving the sale and installation of a customized smart home system because the predominant purpose of the transaction was for the sale of goods.²²² The court compared the cost of the services to the cost of the equipment, the nature of the seller's business and the intent of the parties.²²³ Similarly, in *Triangle Underwrites, Inc.*

218. *Id.* at 433 (noting that the parties "bargained primarily for the right to mass-market the product not for the right to install single copies of the display driver onto their own PCs," and the difference between a licensing agreement and a mass-production agreement); *see also* *Attachmate Corp. v. Health Net, Inc.*, NO. C09-1161 MJP, 2010 U.S. Dist. LEXIS 114445 (W.D. Wash. Dec. 16, 2010) (finding that the UCC did not apply to a breach of contract dispute involving an end user licensing agreement as "the weight of authority favors application of common law and not the UCC with regard to software licenses").

219. 433 F. Supp. 2d 1058 (N.D. Cal. 2006).

220. *Id.* at 1062.

221. 403 S.W.3d 789 (Tenn. Ct. App. 2012).

222. *See id.* at 799–805 (examining the four factors of the predominant purpose test and finding the installation services to be incidental to the actual purpose of the transaction: selling an expensive smart home system).

223. *See id.* at 799–800 (focusing on the number of times the contract referred to the sale of equipment, goods, and hardware). Other courts have also applied the predominant purpose test to hybrid software transactions. *See* *RRX Indus., Inc. v. Lab-Con, Inc.*, 772 F.2d 543, 546 (9th Cir. 1985) (examining the contractual significance of the sold software, training, systems repairs, and upgrades); *Surplus.com, Inc. v. Oracle Corp.*, 2010 U.S. Dist. LEXIS 136254, at *8–11 (N.D. Ill. Dec. 23, 2010) (applying predominant purpose test and holding that Article 2 applies to a software development agreement); *NMP Corp. v. Parametric Tech. Corp.*, 958 F. Supp. 1536, 1542 (N.D. Okla. 1997) (applying the predominant purpose test and holding that Article 2 applied to an engineering software license agreement); *Camara v. Hill*, 596 A.2d 349, 351 (Vt. 1991) (applying the test to a contract for a computer system); *USM Corp. v. Arthur D. Little Sys., Inc.*, 546 N.E.2d 888, 894 (Mass. App. Ct. 1989) (applying the predominant purpose test to a contract to develop and install a turnkey computer system); *Nelson Business Equip. Ctr., Inc. v. Monteleone*, 524 A.2d 1172, 1174 (Del. 1987) (looking at the predominant purpose of a lease contract for software, hardware, and services).

v. Honeywell, Inc.,²²⁴ applying the predominant purpose test, the court found that Article 2 applied to a transaction involving the sale of a computer system consisting of “hardware, or the core computer, printer, collator, and related equipment; ‘software,’ the designation for programming created for use in connection with the hardware; standard programming aids; and ‘custom application software’ specifically designed for [the plaintiff’s] individual needs.”²²⁵

Even if one believes that existing case law supports the conclusion that Article 2 applies to the sale of IOT devices along with the accompanying services and software, in cases applying the predominant purpose test, “for the most part, courts state the facts and then declare an answer, without providing an analysis that is useful to other facts.”²²⁶ This lack of clarity in the case law, combined with the complex nature of IOT devices that rely heavily on services and software provided and maintained by companies, justifies movement towards a new framework.

Software transactions involving the provision of support services could also be viewed solely as service contracts, particularly where software is not being delivered through a physical medium or downloaded, but rather access is made available only through a website. Such transactions are typically governed by “Software as a Service Agreements” with the software being provided through cloud computing.²²⁷ In such an instance, one could contend that the software is not movable at the time of contracting and therefore does not meet the definition of goods under Article 2. Software provided by IOT manufacturers could be viewed as services because software related to the function of the device may be provided through

224. 604 F.2d 737 (2d Cir. 1979).

225. *Id.* at 738.

226. RUSH & SEPINUCK, *supra* note 120, at 4; *see* Braucher, *supra* note 203, at 244 (noting that courts applying Article 2 to software transactions routinely fail to state whether they are applying Article 2 directly to the transaction or simply using it as persuasive authority).

227. Holly K. Towle, *Enough Already: It Is Time to Acknowledge that UCC Article 2 Does Not Apply to Software and Other Information*, 52 S. TEX. L. REV. 531, 547 (2011).

cloud infrastructure. To the extent that IOT software is built into IOT devices and buyers are downloading software updates to their IOT devices, IOT hybrid transactions may be distinct from standard “software as a service” transactions. However, as previously noted, many IOT devices depend not only on software embedded within the device to function but also on cloud computing.²²⁸

Where software transactions are accompanied by the provision of services, at least one court has applied Article 2 to a transaction where the services provided are not “substantially different from those generally accompanying package sales of computer system contracts,” such as installation, training, and technical support services.²²⁹ The services provided in connection with the sale of IOT devices are distinct from these types of traditional software services. Software installation, training, and technical support services are frequently performed by an individual rather than a device.²³⁰ Goods may be able to function even where an owner is not provided with installation or training services. In contrast, IOT software updates and online application services are often critical to the functioning of IOT products. As discussed in Part I, the Revolv IOT device was rendered inoperable after the manufacturer elected to terminate all supporting services and software updates.

As many courts have acknowledged, “[s]oftware is not clearly a good or a service in the abstract, and may qualify as either [a good or a service] depending on the particular circumstances of the case.”²³¹ Most courts view transactions

228. David Linthicum, *The Cloud and the Internet of Things Are Inseparable*, INFOWORLD (Jan. 12, 2016), <http://www.infoworld.com/article/3021059/cloud-computing/cloud-and-internet-of-things-are-inseparable.html> (last visited Mar. 5, 2017) (predicting a significant increase in cloud-based device services) (on file with the Washington and Lee Law Review).

229. See generally *Dahlmann v. Sulcus Hosp. Techs. Inc.*, 63 F. Supp. 2d 772 (E.D. Mich. 1999); *Dealer Mgmt. Sys. v. Design Auto. Grp., Inc.*, 822 N.E.2d 556 (2005).

230. See *Dealer Mgmt. Sys.*, 822 N.E.2d at 561 (“Contracts for the sale of software often also involve the provision of services.”).

231. See *Rottner v. AVG Techs. USA, Inc.*, 943 F. Supp. 2d 222, 230 (D. Mass. 2013) (reasoning that Article 2 applied because the buyer was able to download

involving the transfer of standardized software on a computer disc as a transaction in goods.²³² Despite case law suggesting that the transfer of standardized software qualifies as a good, in the IOT context the services provided in connection with the sale of the device complicate the analysis of whether Article 2 should apply to such transactions.

Where an IOT transaction does not involve the sale of standardized software but rather a corporate software transaction, the provision of software and services may be even more complex and the accompanying software that is specially designed for the company could be viewed as a service and a license rather than a sale of goods subject to Article 2.²³³ Moreover, despite the increased dominance of software in connection with the sale of devices, unlike software sold on a computer disc, IOT devices are much more than the medium through which software is provided. IOT devices are dynamic objects built to actively interact with other devices, their owners, and the environment, and to perform specific functions, such as measuring consumption rates and purchasing goods on behalf of their owners.²³⁴ IOT products are also designed to adapt to their environment to accommodate the needs of their owners.²³⁵

the software). *But see* Specht v. Netscape Commc'ns. Corp., 306 F.3d 17, 29 n.13 (2d Cir. 2002) (noting that Article 2 may not apply to the licensing of software that is downloadable from the internet).

232. *See Rottner*, 943 F. Supp. 2d at 230 (noting that most courts classify any software package as a good).

233. *See* RESTATEMENT (THIRD) OF TORTS § 19 cmt.(d) (1997) ("Under the [U.C.C.] software that is mass-marketed is considered a good . . . However, software that was developed specifically for the customer is a service."); *see also* Simulados Software, Ltd. v. Photon Infotech Private, Ltd. 40 F. Supp. 3d 1191, 1201 (N.D. Cal. 2014) (noting that many courts have "determined that certain software transactions are better defined as services . . . Where software is designed from scratch. . . the software is often found to be a service rather than a good"); WHALEY & MCJOHN, *supra* note 216 (noting that whether Article 2 applies to a transaction involving software is a thorny issue).

234. *See* Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (May 13, 2014), <http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#608dc89a6828> (last visited Mar. 5, 2017) (explaining what IOT is and its many potential applications) (on file with the Washington and Lee Law Review).

235. *See id.* (detailing the anticipatory nature of IOT devices).

Given this level of interactivity, one could contend that IOT devices are no different from video games—which are also designed to interact with players. IOT technology is distinct from traditional video games and it has enhanced the gaming industry. The IOT

has fueled technological innovation in gaming and has changed the way players used to play, now the games are more interactive [and] use artificial intelligence . . . with Tangible User Interface (TUI) i.e. the use of physical sensors [which has led to the creation of] pervasive and mixed reality games that ha[ve] smoothen[ed] [the] playing experience.²³⁶

In the IOT setting multiple devices, such as smartphones, tablets, and other IOT devices, are connected, and this permits players to play, pause, and restart video games “on the go” without the use of video consoles.²³⁷ The makers of Wii and Xbox, for example, are expected to leverage IOT technology to “penetrate the traditional boundaries of gaming” and, ultimately, take the gaming industry to the next level.”²³⁸

Additionally, courts should be wary of analogizing IOT devices to the sale of standardized software on computer discs. Such similarities should not be the basis for applying Article 2 to a transaction. If developers of IOT devices begin to provide software solely through cloud computing and software as a service contracts, the software is no longer on a medium—the IOT device. As a result, these transactions would not be subject to Article 2 under the computer-disc medium rationale.

236. Ashish Mahendra, *How the Internet of Things Revolutionizes the Gaming Industry*, IOTWORM (Nov. 22, 2015), <http://iotworm.com/internet-of-things-changes-gaming-industry/> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

237. See generally Deendayal Choudhary, Ganesh Kutty, Kaustubh Deshpande, Rechana Nadar & Sumit A. Hirve, *Internet of Things—Changing The Game*, 12 INT’L J. SCI. & TECH. RES. 238 (2015).

238. Mahendra, *supra* note 236.

D. Software and Other Sources of Law

The ALI and the National Conference of Commissioners on Uniform State Laws (ULC) first attempted to address software transactions via Article 2B of the UCC.²³⁹ This proposed revision to the UCC subsequently became UCITA after the ALI withdrew from the project.²⁴⁰

UCITA, a proposed uniform law, applies to computer information transactions.²⁴¹ The official comments to UCITA suggest that the model law adopts a gravamen of the action standard with respect to transactions involving goods and computer information.²⁴² UCITA may also apply to software transferred with goods where the goods are a computer or a computer peripheral.²⁴³ As Professors Koopman and Kaner have noted, Internet-enabled goods may qualify as computer peripherals under UCITA because they are connected to a

239. See Juliet M. Moringiello & William L. Reynolds, *What's Software Got To Do with It? The ALI Principles of the Law of Software Contracts*, 84 TUL. L. REV. 1541, 1544 (2010) (providing the history of the ALI's work in this area).

240. *Id.* at 1543.

241. Uniform Computer Information Transactions Act § 103(a) (2002). Certain transactions are excluded from the scope of the model law, such as financial services and insurance transactions, a motion picture or audio or visual programming

other than a mass-market transaction or a submission of an idea or information or release of informational rights that may result in making a motion picture or similar information product; or a sound recording, musical work, phonorecord or an enhanced sound recording, other than in the submission of an idea or information or release of informational rights that may result in the creation of such material or a similar information product.

Id. § 103(d).

242. *Id.* § 103 cmt. 4(b)(1) (noting that the law applicable to an issue depends on whether the issue pertains to goods or computer information and UCITA applies only to the computer information portion of the hybrid transaction, while Article 2 applies to the goods aspect of the transaction). See also *id.* § 103(b)(1) (2002); *id.* § 103 cmt. 4(b)(3). However, the comments to UCITA also refer to a heightened version of the predominant purpose test for other types of mixed transactions. *Id.* § 103 cmt. 4(c).

243. *Id.* § 103(b)(1)(a). UCITA can also cover transactions involving goods and computer information where “giving the buyer or lessee of the goods access to or use of the program is ordinarily a material purpose of transactions in goods of the type sold or leased.” *Id.* § 103(b)(1)(B).

computer either directly or indirectly via a network.²⁴⁴ However, UCITA's impact on IOT transactions involving computer information is limited as it has not been broadly adopted by states and some states have enacted shelter provisions to prevent application of the act.²⁴⁵ Although UCITA contains provisions regarding a right of return that may be applicable in specific circumstances in mass-market license transactions, the model law has faced significant opposition from consumer protection advocates.²⁴⁶ Additionally, the official comments to UCITA suggest that its coverage does not extend to software embedded within goods where "the embedded program is a mere part of the goods."²⁴⁷ Software is likely to be routinely embedded within IOT devices and one could certainly contend that the software embedded within such devices is an indistinguishable part of the device.

244. PHILIP KOOPMAN & CEM KANER, THE PROBLEM OF EMBEDDED SOFTWARE IN UCITA AND DRAFTS OF REVISED ARTICLE 2 (2001), <http://kaner.com/pdfs/embedd1.pdf> (explaining that Internet-enabled household appliances could qualify as computer peripherals, due to the difficulty of defining computer peripherals in a practical manner); see also Cem Kaner, *Uniform Computer Information Transactions Act: Software Engineering and UCITA*, 18 J. MARSHALL J. COMPUTER & INFO. L. 435, 525 (1999) (stating that "if a copy of a program is contained in and sold or leased as part of a computer or computer peripheral . . . then the program is within the scope of UCITA under section 103(b) and the vendor can bring the whole transaction . . . under UCITA"). But see Linda Rusch, *Is the Saga of the Uniform Commercial Code Article 2 Revisions Over? A Brief Look at What NCCUSL Finally Approved*, 6 DEL. L. REV. 41, 45 (2003) (suggesting that smart goods are not computer peripherals).

245. Elvy, *supra* note 19, at 887. To date, only Maryland and Virginia have adopted the UCITA. *Legislative Fact Sheet—Computer Information Transactions Act*, UNIFORM L. COMM'N, http://www.uniformlaws.org/Legislative_Fact_Sheet.aspx?title=Computer%20Information%20Transactions%20Act (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review); see also IOWA CODE § 554D.104 (2015); N.C. GEN. STAT. § 66-313 (2015); W. VA. CODE § 39A-1-1 (2015).

246. Uniform Computer Information Transactions Act § 209(b) (2002). See generally Robert Oakley, *Fairness in Electronic Contracting: Minimum Standards for Non-Negotiated Contracts*, 42 HOUS. L. REV. 1041, 1073 (2005).

247. Uniform Computer Information Transactions Act § 103 cmt. 4(b)(3) (2002) ("[UCITA] does not apply to a copy of a program on a computer chip embedded as part of an automobile engine and sold or leased as an indistinguishable part of the automobile containing the engine. On the other hand, [UCITA] does apply to a copy of a program contained on a computer chip in a computer and transferred along with the computer.").

The Software Principles represent the ALI's second effort to unify the law of software agreements. Proponents of the Software Principles have argued that software transactions are different from transfers of goods and therefore, Article 2 and the common-law are not equipped to address such transactions.²⁴⁸ As previously noted, the software embedded within an IOT device is likely to be governed by an EULA.²⁴⁹ The Software Principles apply to software agreements supported by consideration, including licenses, sales, and access contracts, and it provides that contract formation issues should be evaluated by using a reasonableness standard.²⁵⁰

The Software Principles provide that a software agreement term is unenforceable where it conflicts with a mandatory rule or the purposes and policies of intellectual property law, or would constitute misuse in an infringement proceeding.²⁵¹ Further, to protect buyers in transactions involving the purchase of defective software, the Software Principles provide for an implied warranty of no material hidden defects that cannot be disclaimed.²⁵² The warranty is based on the duty of good faith, the duty to disclose, and fraudulent-concealment law.²⁵³ In consumer agreements and standard form transfers of generally available software, the Software Principles prohibit a transferor from disabling the software as a remedy for breach of

248. See, e.g., Raymond T. Nimmer, *Through the Looking Glass: What Courts and UCITA Say About the Scope of Contract Law in the Information Age*, 38 DUQ. L. REV. 255, 257–58 (2000) (arguing that neither Article 2 nor the common law are suited to regulate software transactions).

249. *Terms of Service*, NEST, *supra* note 76. Nest users are subject to an EULA for software associated with Nest devices. *Id.*

250. SOFTWARE PRINCIPLES, *supra* note 44, §§ 1.06(a), 2.02.

251. See *id.* § 1.09 (providing for the consideration of intellectual property law).

252. See *id.* § 3.05(b) (prohibiting implied warranty of no material hidden defects from being disclaimed); see also Robert Hillman, *Contract Law in Context: The Case of Software Contracts*, 45 WAKE FOREST L. REV. 669, 677 (2010) (discussing the nondisclaimable warranty of no hidden material defects of which the transferor is aware).

253. See SOFTWARE PRINCIPLES, *supra* note 44, § 3.05 cmt. b. (detailing the warranty's foundational principles and legal authority).

the agreement regardless of whether the contract contains a conspicuous automatic disabling provision.²⁵⁴

Despite the potential protections provided to transferees under the Software Principles, the application of the Software Principles to hybrid IOT transactions is questionable. First, the Software Principles are soft law, which courts and parties are free to ignore.²⁵⁵ Second, the Software Principles exclude the transfer of disks, CD-ROMs, “or other tangible medium that stores the software” and embedded software in goods where the predominant purpose of the transaction is for the sale of goods rather than software.²⁵⁶ As discussed in Part III.A above, while hybrid IOT transactions are distinct from contracts involving the transfer of software on computer discs, software is frequently built into IOT devices.

To the extent that software is embedded within an IOT device and a court concludes that the predominant purpose of the transaction is for the transfer of software rather than goods, the Software Principles may apply to the transaction.²⁵⁷ With a few exceptions, the comments of the Software Principles indicate that the factors that courts have used in the Article 2 context to apply the predominant purpose test should also be used in deciding the Software Principles’ applicability to hybrid software transactions.²⁵⁸ As with the traditional predominant

254. *Id.* § 4.03(c), (d); *see also* Hillman, *supra* note 252, at 675 (noting that the Software Principles “balance the interests of transferors and transferees and authorize automated disablement in limited circumstances and only after receiving court authorization”). *But see* SOFTWARE PRINCIPLES, *supra* note 44, § 4.03(d) (noting that automated disablement is permitted in certain instances).

255. Michael L. Rustad & Maria Vittoria Onufrio, *The Exportability of the Principles of Software: Lost in Translation?*, 2 HASTINGS SCI. & TECH. L.J. 25, 43–44 (2009).

256. SOFTWARE PRINCIPLES, *supra* note 44, §§ 1.06(b)–1.08; *see also* Hillman, *supra* note 252, at 673 (noting that the Software Principles exclude embedded software unless, measured objectively, the predominant purpose of the transferee is to obtain the software).

257. *See* SOFTWARE PRINCIPLES, *supra* note 44, § 1.07(a) (excluding embedded software unless the predominant purpose of the transferee is to obtain the software).

258. *See id.* § 1.07 cmt. b (listing language of the agreement; nature of goods; price of goods; nature of parties’ bargaining; ease of copying and transferring; general availability of the software; whether there is a separate price for the

purpose test, no specific factor is controlling under the Software Principles. Where non-embedded software is provided along with “any combination of goods, digital content and services,” the Software Principles suggest that it applies to the software aspect of the transaction “unless the services or digital content predominate.”²⁵⁹ The Software Principles’ retention of the predominant purpose test to assess its applicability to hybrid transactions involving the sale of goods and software is problematic given the deficiencies of the predominant purpose test noted in Part III.A above.

The ALI has described the purpose of the Software Principles as aimed at describing the law of software contracts as it should be.²⁶⁰ The Software Principles have been criticized for failing to provide clear guidance on distinguishing between a license and a sale while addressing generic issues, such as unconscionability.²⁶¹

The Software Principles have also been criticized for failing to clearly cover digital content.²⁶² As Professor Kim notes, software is often viewed as a subset of digital content and “digital content is often bundled with embedded software in

software; and whether the transferor developed the software for the particular transferee or product as factors).

259. *Id.* at 1–2 Summary Overview, § 1.07 cmt. d, § 1.08.

260. *See id.* § 1.07 cmt. B (criticizing and rejecting UCITA’s material purpose test).

261. *See Moringiello & Reynolds, supra* note 239, at 1546–47 (questioning the reasons for leaving out such guidance in light of the work’s aspirational nature).

262. *See* Nancy S. Kim, *Expanding the Scope of the Principles of the Law of Software Contracts to Include Digital Content*, 84 TUL. L. REV. 1595, 1595 (2010) [hereinafter Kim, *Expanding the Scope*] (contending that the Software Principles should encompass digital content because distinguishing digital content from software may be difficult for courts and the exclusion of such content fails to resolve the conundrum of how to balance the proprietary rights and interests of licensor-owners and the rights and interests of licensee-consumers). The Software Principles define digital content as “digital art,” which is “literary and artistic information stored electronically, such as music, photographs, motion pictures, books, newspapers, and other images and sounds,” and “digital database,” which is a “compilation of facts arranged in a systematic manner and stored electronically.” SOFTWARE PRINCIPLES, *supra* note 44, § 1.01(f)(2). The predominant purpose test also applies to hybrid transactions involving digital content and software. *Id.* § 108.

multimedia products.”²⁶³ As a result, it may be difficult for courts to distinguish between digital content and software.²⁶⁴ This problem may be exacerbated as disruptive IOT technology becomes ubiquitous and digital content is more easily integrated with software and IOT devices. The Software Principles also provide a safe harbor provision that upholds electronic form contracts and binds transferees where a transferee has reasonable notice of and access to contract terms prior to payment, and indicates agreement to the terms at the end of or adjacent to the electronic form contract, among other things.²⁶⁵ This standard likely validates clickwrap agreements.²⁶⁶ As I have argued elsewhere, restrictive notions of notice and an opportunity to review are inadequate for consumer IOT contracts.²⁶⁷

A consumer who owns an IOT device may be provided with what is arguably reasonable notice of contract terms prior to associating or registering the device to purchase goods and supplying credit card information to enable the device to place subsequent orders on their behalf.²⁶⁸ Terms of use may also be supplied to a consumer upon establishing an account with a retailer or a link may be provided to the conditions of use

263. Kim, *Expanding the Scope*, *supra* note 262, at 1603–06.

264. *See id.* at 1595–96, 1603–04 (arguing that consumers do not distinguish between digital content and software). For instance, “while a reader may distinguish a Kindle from an e-book, he or she probably does not think about the words separately from the software that enables the words to be displayed.” *Id.* at 1604.

265. SOFTWARE PRINCIPLES, *supra* note 44, § 2.02(c).

266. In a clickwrap agreement, a buyer is required to click an “I agree” button after the terms of the agreement are disclosed. RUSCH & SEPINUCK, *supra* note 120, at 60.

267. *See* Elvy, *supra* note 19, at 846–49 (contending that high levels of information asymmetry and contract distancing should be considered when evaluating consumer assent to contract terms in the IOT setting). Other scholars have also highlighted concerns with the use of one-sided legal provisions in consumer contracts in the non-IOT context. *See, e.g.*, Amy Schmitz, *Access to Consumer Remedies in the Squeaky Wheel System*, 39 PEPP. L. REV. 279, 281 (2012) (discussing the ways in which companies “capitalize on continued freedom to impose fees and one-sided contract terms” on uninformed consumers).

268. *See* Elvy, *supra* note 19, at 852 (describing the general characteristics and functions of IOT devices).

whenever a consumer proceeds through the login process. However, a consumer may not be provided with contract terms or even amended contract terms prior to the device placing a sixth or seventh order for goods, and a consumer may not always be required to access hyperlinks containing the terms and conditions as part of the login process.²⁶⁹ Because the consumer was given reasonable notice of the contract terms prior to registering the device to place orders, the consumer could be bound to provisions that are detrimental to his or her ability to seek legal redress.²⁷⁰ This standard does not adequately address the failure of consumers to read and understand contract terms, which continues to be a pressing problem.²⁷¹ Consider that Amazon's DRS terms and conditions provide that its liability for each claim is limited to fifty dollars.²⁷² Further, IOT devices allow consumers to mindlessly purchase goods without reflection, thereby increasing the ease with which consumers can become further indebted to credit card companies and other creditors.²⁷³

IV. Proposals

The goals of substantive uniformity, clarity, and simplicity are central to the UCC.²⁷⁴ One of the central aims of the ULC

269. See *id.* at 844 (“The consumer is not required to access the company’s website or mobile application (which contains contract terms), review the company’s terms or conditions, or click an ‘I agree’ button before each subsequent order is placed.”).

270. See *id.* at 879 (noting that courts may infer a consumer’s notice of contract terms because the terms may have been provided when the IOT device was first activated).

271. See *id.* at 874 (citing statistics from multiple cases and studies which show that consumers routinely fail to read contract terms).

272. See *Amazon Dash Replenishment Terms of Use*, *supra* note 57 (“IN NO EVENT WILL OUR OR OUR LICENSORS’ AGGREGATE LIABILITY UNDER THIS AGREEMENT WITH RESPECT TO ANY CLAIM EXCEED FIFTY DOLLARS (\$50.00).”).

273. See Elvy, *supra* note 19, at 878 (explaining how mindless purchasing further distances consumers from contract terms). My future scholarship in this area will continue to explore the relationship between automated consumer debt and the new IOT contracting environment.

274. See U.C.C. § 1-103 (AM. LAW INST. & UNIF. LAW COMM’N 2002)

was to encourage states to enact uniform acts to prevent federal intervention in the wake of the Supreme Court's decision in *Swift v. Tyson*.²⁷⁵ In 1945, the ALI began working with the ULC to draft the UCC in an effort to eliminate previous piecemeal adoption of uniform legislation by states.²⁷⁶ By 1975, the UCC had been adopted in every American state with Louisiana adopting only specific articles of the UCC.²⁷⁷

Given the potential imperfections in state processes for adoption and enforcement of the UCC, the use of local amendment to vary the text of the UCC, and a lack of clarity or silence in the UCC in some areas, the goal of uniformity has proved to be elusive.²⁷⁸ Article 2's failure to provide explicit guidance on how best to handle hybrid transactions involving goods, services, or software is one such area in which a lack of harmony and uniformity continues to be rampant and is likely to be problematic in the age of the IOT. Rather than achieving substantive uniformity among states, the UCC has instead facilitated consensus on certain important commercial law issues, a laudable but different goal from the one envisioned by the drafters of the UCC.²⁷⁹

The lack of clarity in UCC case law on how to evaluate hybrid transactions and the potential limited application of common-law warranties, UCITA, and the Software Principles indicate that a new framework in this area is needed. Courts

(enumerating the underlying purpose and policies of the U.C.C.).

275. See Taylor, *supra* note 3, at 529 (pointing to concern over the Supreme Court's decision in *Swift* to apply the general law of commerce rather than state law in commercial law cases); see also *Swift v. Tyson*, 41 U.S. 1, 12 (1842) ("Undoubtedly, the decisions of the local tribunals upon such subjects are entitled to, and will receive, the most deliberate attention and respect of this court; but they cannot furnish positive rules, or conclusive authority, by which our own judgments are to be bound up and governed."), *overruled by* *Erie R. Co. v. Tompkins*, 304 U.S. 64 (1938).

276. See Taylor, *supra* note 3, at 530 ("The sponsor hoped through consolidation to sell the whole package to the various states and thus avoid some of the 'picking and choosing' in which the states had engaged with earlier uniform acts.").

277. *Id.* at 531.

278. See *id.* (summarizing the various factors that led to a lack of uniformity by states in applying the Uniform Commercial Code).

279. See *id.* at 531 ("[L]ikeness rather than exactness—harmony rather than uniformity—has been the history of the 'Uniform' Commercial Code . . .").

should abandon the predominant purpose test which has led to conflicting decisions in cases involving similar facts. Four potential proposals for increasing clarity and uniformity in this area include: (1) expanding the scope of Article 2 to cover transactions involving “products,” (2) adopting a functionality test that evaluates the relationship between the goods, software, and services, (3) adopting Article 9’s definition of goods, and (4) excluding such transactions from the scope of Article 2. The remainder of this section evaluates the efficacy and potential drawbacks of each proposal. The Article concludes by calling for the adoption of the functionality approach.

A. Products Approach

One approach to improving clarity in assessing hybrid transactions is to widen the scope of Article 2 to cover not only transactions in goods, but also transactions involving products. This would include the hardware of IOT devices, embedded software, software updates, and other related services and software provided by a retailer or manufacturer. Under this approach, a seller and a buyer of an IOT device will know in advance that the entire transaction, including the software and the services, will be subject to Article 2. This avoids unnecessary litigation about Article 2’s applicability to such transactions. Other provisions of Article 2 which may arguably be limited to a contract for the sale of goods may also need to be amended to give full effect to this solution.

The IOT is expected to usher in an era in which almost every movable item can be designed with “electronics, software and sensors and connectivity that allow these objects to collect and exchange data.”²⁸⁰ Further, the industrial IOT will transform manufacturing goods into “systems of intelligence.”²⁸¹ General Electric estimates that by 2020 revenues from the industrial

280. Tim Maverick, *The Future of the Industrial Internet of Things*, TREFIS (May 6, 2016), <http://www.trefis.com/stock/spy/articles/354034/the-future-of-the-industrial-internet-of-things/2016-05-06> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

281. *Id.*

IOT will be \$225 billion and \$170 billion for the consumer IOT.²⁸² Goods will cease to be the static objects that Article 2 was drafted to initially cover. The services and software provided by manufacturers and retailers in connection with the transfer of an IOT device allow these devices to operate as goods. In other words, but for the service and the related software, there would be no good. The sale of an IOT device is much more than a simple transfer of moveable hardware from seller to buyer. Such an agreement involves a complex transaction comprising of the transfer of hardware, embedded software, and the expected provision of ongoing services and software updates. If all goods are now Internet-enabled and are accompanied by ongoing services and software, limiting Article 2's scope to the static goods of the pre-information era simply fails to consider this new reality.

There are potential concerns with expanding Article 2's scope to cover transactions involving "products." First, one could argue that Article 2 is not the best body of law to govern disputes involving IOT transactions. Article 2 does not clearly address all issues related to software transactions, such as the role of federal intellectual property law²⁸³ and the distinction between the license and sale of software.²⁸⁴ However, the application of Article 2 to an IOT transaction does not prevent the application of federal intellectual property law. Transactions involving software embedded within goods are less likely to raise intellectual property issues regarding "copying, transfer, support, maintenance, upgrade, inspection, monitoring,

282. See *id.* (noting that venture investment into industrial IOT has grown by 76% to over \$1 billion).

283. See David Nimmer, Elliot Brown & Gary N. Frischling, *The Metamorphosis of Contract into Expand*, 87 CAL. L. REV. 17, 19 (1999) (examining the later-rejected Article 2B of the U.C.C. and federal copyright law). The subsequent sale of an IOT device from one consumer to another may also raise interesting intellectual property, questions and my future work in this area will explore such issues.

284. See Abby J. Hardwick, Note, *Amending the Uniform Commercial Code: How Will a Change in Scope Alter the Concept of Goods?*, 82 WASH. U. L. REV. 275, 285 (2004) (recognizing the Business Software Alliance's proposal to draft a new U.C.C. article to govern software contracts given that computer information generally takes the form of a conferred license).

licensing restrictions, or remedial limitations (in any way distinct from the goods themselves).”²⁸⁵ Software prebuilt into goods may be more difficult to copy and interoperability issues in the IOT setting may prevent any such software from being freely copied, transferred, and used in another brand or type of goods.²⁸⁶ Additionally, given UCITA’s limited reach and the soft-law status of the Software Principles, Article 2 remains the better alternative.

Second, the adoption of such an expansive approach could result in Article 2 applying to every aspect of a hybrid transaction even if the predominant purpose of the transaction is not for the sale of goods but for the provision of services or software. This arguably contradicts section 2-102, which limits Article 2’s application to transactions in goods.²⁸⁷ Automatic application of Article 2 to a hybrid transaction may be detrimental to purchasers in some instances. Article 2 imposes a four-year statute of limitations, which may be shorter than the period applicable under other sources of law, and permits parties to reduce the limitations period to not less than one year.²⁸⁸ Additionally, many of Article 2’s provisions can be

285. Robert Hillman, *Principles of the Law of Software Contracts*, 2010 A.L.I. 1, 2.

286. *See id.* (“[E]mbedded software typically is difficult to copy and special-purpose in nature . . .”).

287. U.C.C. § 2-102 (AM. LAW INST. & UNIF. LAW COMM’N 2002).

288. *Id.* § 2-725. A cause of action generally accrues when the breach occurs regardless of the aggrieved party’s lack of knowledge of the breach and a breach of warranty occurs when tender of delivery is made. *Id.* § 2-725(2). However, if the seller’s warranty explicitly extends to the future performance of the good and discovery of the breach must await the time of such performance, the cause of action accrues when the breach is or should have been discovered. *Id.* Article 2 explicitly preserves tolling of the statute of limitations. *Id.* § 2-725(4). In *Perlmutter v. Don’s Ford, Inc.*, the court held that Article 2 did not apply to the transaction and as such a six-year statute of limitations applied to the transaction. *See generally* 409 N.Y.S.2d 628 (City Ct. 1978) (determining that the four-year Statute of Limitations under § 2-725 of the U.C.C. did not apply). Additionally, a seller’s statute of fraud defense, as well as risk of loss rules, may be detrimental to a buyers’ claim. NAT’L CONSUMER LAW CTR., *supra* note 136, at 164. While other sources of law, including the common law, may uphold contracts that reduce the statute of limitations, some courts have imposed a reasonableness requirement in evaluating the validity of such contracts in the non-Article 2 context. *See Beck v. General Ins. Co.*, 18 P.2d 579, 583 (Or. 1933) (finding that “there is nothing in the policy [of statutes of limitation] or object of such statutes

varied by contract. If Article 2 applies to the hybrid transaction, sellers would still be permitted under Article 2 to disclaim implied warranties and extend express warranties only to the device and not to the services or software.²⁸⁹ To address this concern, the Warranty Act's approach, which prevents the disclaimer of implied warranties where a written warranty has been provided, could be adopted.²⁹⁰

I have argued elsewhere that there are specific areas of Article 2 that are in need of improvement in the IOT setting, and I have proposed amendments to Article 2 to alleviate these concerns.²⁹¹ However, in the absence of a statute that is designed to address the sale of IOT products consisting of a device and ongoing online services and software, Article 2 is perhaps the most sensible alternative. Article 2 is the main uniform body of state law currently available to address transactions in goods.

Third, rather than Article 2 applying to the entire transaction, one could posit that it is best to apply multiple and separate sources of law that are designed to address specific aspects of IOT hybrid transactions. Following this line of reasoning, Article 2 and the Warranty Act could apply to the sale of the device's hardware, while the common law and the Warranty Act govern the service agreement,²⁹² and the Software Principles, the common law or UCITA, and intellectual property law apply to the EULA. This approach is similar to the component test, where Article 2 is applied only to the goods aspect of the transaction.²⁹³ However, consider a consumer who

which forbids the parties to an agreement to provide a shorter period, provided the time is not unreasonably short").

289. See U.C.C. § 2-316 (AM. LAW INST. & UNIF. LAW COMM'N 2002) (outlining available exclusions and modifications to warranties).

290. See Magnuson-Moss Warranty-Federal Trade Commission Improvement Act, Pub. L. No. 93-637, § 108(A), 88 Stat. 2183 (1975) (codified at 15 U.S.C. § 2308(a) (2012)) ("No supplier may disclaim or modify . . . any implied warranty to a consumer with respect to such consumer product if (1) such supplier makes any written warranty to the consumer with respect to such consumer product . . .").

291. See generally Elvy, *supra* note 19.

292. Depending, of course, on whether the service agreement qualifies as a service contract under the Warranty Act.

293. See generally *supra* note 135.

has purchased an IOT device who discovers that, in order to use the device as advertised by the manufacturer or retailer, she will be subject to three separate contracts that are governed by four or five different sources of law. As I have noted elsewhere, consumers frequently fail to read and understand contract terms.²⁹⁴ Thus, consumers are unlikely to spend time attempting to understand three separate contracts and the many distinct sources of law that may govern their rights under each contract. Application of this approach would lead to more than one source of law governing a hybrid transaction and this could present insurmountable problems of proof in determining how to apply different rules of damages.²⁹⁵

B. Functionality Approach

Alternatively, a functionality test could be adopted to assess whether hybrid IOT transactions fall within the scope of Article 2. In IOT hybrid transactions, the services and software are no longer “merely incidental to the sale of [the] goods.”²⁹⁶ Rather, the software and services constitute an integral part of the device’s operations as evidenced by the Revolv smart hub’s lack of functionality after services were terminated by the company as discussed in Part I above.²⁹⁷ Similarly, glitches in the required automatic software updates for the Nest Learning Thermostat have left “the thermostat unresponsive, unable to control heating systems and often drained of all power.”²⁹⁸

294. See Elvy, *supra* note 19, at 874 (“Consumers routinely fail to read contract terms.”)

295. See Hudson v. Town & Country True Value Hardware, Inc., 666 S.W.2d 51, 54 (Tenn. 1984) (“[T]he majority of sales . . . consisting of both goods and non-goods, would present difficult and in some instances insurmountable problems of proof in segregating assets and determining their respective values at the time of the original contract and . . . resale, in order to apply two different measures of damages”); see also Brush, *supra* note 124, at 14–16.

296. Triangle Underwriters, Inc. v. Honeywell, Inc. 604 F.2d 737, 743 (2d Cir. 1979).

297. *Supra* Part I.

298. Iain Thomson, *Nest Thermostat Owners Out in the Cold After Software Update Cockup*, REGISTER (Jan. 14, 2016, 12:17 AM), http://www.theregister.co.uk/2016/01/14/nest_foul_up/ (last visited Mar. 5, 2017)

Under a functionality approach, where the functionality of the IOT device depends on the provision of services and software to be supplied by the manufacturer or retailer, Article 2 would apply to the entire transaction. If a manufacturer or retailer has advertised the device as being able to perform certain functions and ongoing services, and software updates are needed in order for a purchaser to use all aspects of the device, the transaction should be subject to Article 2. Even where an agreement is labeled as a license of software or services, if the software and services are tied to the operations of the device, Article 2 should govern the related dispute.

Conversely, if a buyer can use all features of the device as advertised by the manufacturer or retailer without the provision of services and software, then Article 2 would apply only to the goods portion of the transaction. This is likely to be rare in the IOT setting. In such an event, different sources of law could apply to the transaction, resulting in a similar problem discussed in Part IV.A above.²⁹⁹ However, the functionality approach more adequately captures the ways in which IOT devices are used and advertised.

In applying the functionality test, courts would evaluate how a device is advertised to buyers by the manufacturer and retailer as well as how integral the services and software are to the operations of the device.

One could argue that the adoption of such a singular approach to hybrid transactions is not preferable. Given the expected evolution of the IOT, it is perhaps beneficial for states and courts to serve as laboratories for experimentation that would generate multiple solutions allowing for the identification of the best approach to dealing with hybrid transactions. However, since the adoption of Article 2, courts have struggled to evaluate hybrid transactions and decades later only two major alternatives have been offered: the predominant purpose test and the gravamen of the claim test.³⁰⁰ Both of these approaches

(on file with the Washington and Lee Law Review). Software glitches have also led to freezing homes and fear of burst water mains. *Id.*

299. *Supra* Part IV.A.

300. *Supra* Parts III.A.1–2.

are problematic as discussed in Part III.³⁰¹ Uniformity of the law among various jurisdictions is one of the central underlying policies of the UCC, and resolving this ambiguity in Article 2 via the adoption of a singular approach, which considers the unique manner in which services and software are provided in connection with the sale of IOT devices, furthers this important goal.

1. Functionality Approach vs. Predominant Purpose Test

Another potential critique of the functionality test is that this approach is no different from the predominant purpose test. However, the functionality approach avoids many of the drawbacks of the predominant purpose test.

First, because the predominant purpose test considers the parties' purpose for entering into the transaction and the terms of the contract, including the label given to the contract by the parties, either party can easily mold their arguments to satisfy the factors of the test. An analysis of the parties' main objective for entering into the underlying transaction likely requires testimony from the parties regarding their reasons for contracting. A buyer could easily claim that its predominant purpose for entering into the transaction was for the purchase of goods rather than services or software. Conversely, a seller could simply label all aspects of a hybrid IOT transaction, including the various contracts, as a license rather than a sale. Cable companies routinely lease rather than sell cable boxes to consumers and these rental fees total approximately \$19.5 billion in revenue annually.³⁰² IOT manufacturers could elect to

301. *Supra* Parts III.A.1–2.

302. See Markey, *Blumenthal Decry Lack of Choice, Competition in Pay-TV Video Box Marketplace*, ED MARKEY, UNITED STATES SENATOR FOR MASSACHUSETTS (July 30, 2015) <http://www.markey.senate.gov/news/press-releases/markey-blumenthal-decry-lack-of-choice-competition-in-pay-tv-video-box-marketplace> (last visited Mar. 5, 2017) (remarking that approximately ninety-nine percent of customers rent their cable box) (on file with the Washington and Lee Law Review). The Federal Communications Commission has proposed new “set-top-box” rules that would force providers to open their services to other companies. See Anthony Wood, *How the FCC’s ‘Set-Top Box’ Rule Hurts Consumers*, WALL ST. J. (Apr. 21, 2016, 7:05 PM), <http://www.wsj.com/articles/how-the-fccs-set-top-box->

do the same. Where IOT devices routinely collect data about buyers, courts should be wary of permitting companies to label transactions as a license or lease rather than a sale as this could remove the transaction from Article 2's scope.

A party with superior bargaining power could also include additional contract language to indicate that the transaction is for the provision of services rather than goods. A seller may also easily contend that, in the IOT setting, the services and software provided by manufacturers and retailers are more valuable to buyers entering into an IOT transaction. As discussed in Part II above, a buyer may elect to purchase an IOT device because of the convenient services provided in connection with the sale of the device.³⁰³ While intending to transfer title of the physical device to the buyer, a seller of such a device is unlikely to contemplate granting the buyer title to the software or services accompanying such a device.

While the functionality test does not ignore the goals of the parties or the expectations of the buyer, this method inserts objectivity into the analysis. The functionality approach evaluates the role of the services and software in the operations of the device and, where the services and software are integral to the operations of the device, they should be viewed as part of the goods and the transaction should be subject to Article 2. If necessary, parties could easily submit evidence regarding advertising materials and the device's operations including its hardware, software, digital content, ancillary updates and services.

The functionality approach eliminates the need for the nuanced, varied, and tedious inquiries performed by courts in applying the predominant purpose test, such as a comparison of the costs of the services and goods, and the nature of the seller's

rule-hurts-consumers-1461279906 (last visited Mar. 5, 2017) (commenting on potential implications of the Federal Communication Commission's "set-top-box" rules) (on file with the Washington and Lee Law Review); *see also* FCC, PROPOSAL TO UNLOCK THE SET-TOP BOX (2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-337449_A1.pdf ("Since 1994 . . . the cost of cable set-top-boxes has risen 185 percent while the cost of computers, televisions, and mobile phones has dropped by 90 percent.").

303. *Supra* Part II.

business. Additionally, under the predominant purpose test, the expectation of the buyer is one of many factors that courts may evaluate and courts do not provide guidance on which specific factor should be more heavily considered as discussed in Part III above.³⁰⁴ The functionality method avoids the pitfalls of the excessive multifactor approach of the predominant purpose test.

Second, although the functionality approach considers the manner in which the IOT device was advertised to buyers, products must be advertised to attract buyers. Currently, IOT manufacturers frequently advertise all features of IOT devices.³⁰⁵ In explaining the convenience of such devices, the benefits of the embedded software and software updates that permit the performance of certain functions and the accompanying services are routinely described to purchasers.³⁰⁶ Buyers have become accustomed to and expect this level of specificity in advertising. It is unlikely that retailers or manufacturers will mold their advertising materials to meet the requirements of the functionality test in an effort to avoid the application of Article 2.

Further, because the functionality approach evaluates the operations of the device even if manufacturers were tempted to manipulate advertising materials, the composition and operations of the device speaks for itself. Legal prohibitions on false and deceptive advertising should also serve as a deterrent to any such manipulation.³⁰⁷ In short, the functionality test does not require courts to evaluate multiple vague factors and the functionality test is less susceptible to manipulation by the parties.

304. *Supra* Part III.

305. *See Meet the Nest Thermostat*, NEST, <https://nest.com/thermostat/meet-nest-thermostat/> (last visited Mar. 5, 2017) (marketing the varying features of Nest thermostats) (on file with the Washington and Lee Law Review).

306. *See id.* (focusing on the thermostat's ability to collect data about the user's habits).

307. *See* 15 U.S.C. § 52(a) (2012) ("It shall be unlawful for any person, partnership, or corporation to disseminate, or cause to be disseminated, any false advertisement . . ."). Additionally, section 2-102 of the UCC provides that the provisions of Article 2 are not intended to impair or repeal any statute regulating sales to consumers. U.C.C. § 2-102 (AM. LAW INST. & UNIF. LAW COMM'N 2002).

Moreover, a functionality test sufficiently accounts for the types of devices that are generated by the IOT—devices that are Internet-enabled and sold with the assumption that services and software will be needed for the device to properly function. Historically, when goods were accompanied by services, the services were severable or divisible from the operation of the goods.³⁰⁸ The predominant purpose approach, the gravamen of the claim approach and even the component test presume that the services can be separated from the goods.³⁰⁹

In the IOT setting, networks, systems, devices, companies and individuals are all connected, goods are frequently embedded with software, and services are provided through the devices to promote this interconnectivity. Divisibility ceases to exist or at the very least decreases significantly. The services and software are no longer easily severable from the operation of the goods. Further, where a plaintiff alleges economic loss because an IOT device or its accompanying software malfunctions such claims should be heard under Article 2.

2. Functionality Approach vs. Products Approach

An additional possible criticism of the functionality approach is that it is identical to the products approach. Manufacturers include software in goods to serve a purpose and software will frequently be connected to the operations of a device. Following this line of reasoning, under the functionality test all devices containing software would be subject to Article 2—which is similar to the result obtained under the products approach.³¹⁰ One potential response to this critique is that not all software, or software upgrades for that matter, are needed in order for a device to function.

The monetization of software in the IOT setting presents one such example. Consider that, in 2015, Tesla announced a software upgrade to increase the high speed auto-pilot

308. *Supra* Part III.

309. *Supra* Part III.

310. *Supra* Part IV.A.

capabilities of its cars—the Model S—for a cost of \$2,500.³¹¹ The Tesla vehicle could continue to function without the upgrade at the time of contracting because it was an optional feature provided by the company. Similarly, installation and training services which may be provided by an IOT manufacturer are not always central to a device's operations.

3. Cybersecurity and Warranties

Where the functionality of the device depends on the software and services provided by the manufacturer and—as a result of the provision of these products—companies are able to collect and retain data about owners, companies collecting and using this information should be obligated to secure the data and the device. There are no uniform rules governing data breach disputes because states have adopted varying laws on this issue.³¹² For companies doing business in multiple states “the different and confounding state laws make responding to a data breach in an appropriate, timely and compliant fashion very difficult.”³¹³

311. See Aaron M. Kessler, *Tesla Adds High-Speed Autonomous Driving to Its Bag of Tricks*, N.Y. TIMES (Oct. 15, 2015), <http://www.nytimes.com/2015/10/16/automobiles/tesla-adds-high-speed-autonomous-driving-to-its-bag-of-tricks.html?> (last visited Mar. 4, 2017) (“It is the first time that a production vehicle available to consumers will have such advanced self-driving capabilities.”) (on file with the Washington and Lee Law Review).

312. Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 52 (2015) (describing how the scattered approach to addressing privacy has prompted gap filling by states); see also Kevin L. Miller, *What We Talk About When We Talk About “Reasonable Cybersecurity”: A Proactive and Adaptive Approach*, FLA. B.J., Sept.–Oct. 2016, at 23 (contending that the “current U.S. legal framework for cybersecurity is a patchwork, consisting of a number of overlapping federal standards aimed at regulated entities in various sectors, state cyber-breach notification laws, state statutes, and case law arising from consumer’s actions against companies”).

313. Stephen Embry, *State Data Breach Notification Law Just Got crazier*, L. TECH. TODAY, (Apr. 19, 2016) <http://www.lawtechnologytoday.org/2016/04/crazy-quilt-work-state-data-breach-notification-laws-just-got-crazier/> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

Article 2 should play an important role in data breach cases and lawsuits involving insecure IOT devices, particularly where a company provides an IOT device that is vulnerable to intrusion or where a company fails to provide adequate security for the data collected by the device and online services accompanying the device. In such instances, consumer owners of IOT devices should have a cause of action for breach of implied warranties under Article 2. Companies may also need to consider clearly informing consumers about the extent to which services, security patches and software updates will be provided during the life-cycle of the device.

Under the implied warranty of merchantability, goods that are sold by merchants who deal in goods of that kind must be fit for the ordinary purpose for which such goods are used.³¹⁴ The implied warranty of merchantability arises in a contract for sale, and software is normally licensed rather than sold.³¹⁵ Thus, in a hybrid transaction where software, services and goods are provided, one could argue that the implied warranty extends only to the portion of the transaction that constitutes a contract for sale. However, if the ordinary purpose for which IOT devices are used includes the facilitation of interconnectivity and the exchange of data between devices, networks, individuals, and companies, and software and services are needed to achieve this goal, this warranty is breached where a company collecting data

314. See U.C.C. § 2-314(1) (AM. LAW INST. & UNIF. LAW COMM'N 2012) (“[A] warranty that the goods shall be merchantable is implied in a contract for their sale if the seller is a merchant with respect to goods of that kind.”); see also *id.* § 2-314(3) (“[O]ther implied warranties may arise from course of dealing or usage of trade.”). Additional objections to the application of implied warranties to software agreements include the claim that software programs are “diverse collections of ideas that cannot reasonably be compared to one another.” Robert W. Gomulkiewicz, *The Implied Warranty of Merchantability in Software Contracts: A Warranty No One Dares to Give and How to Change That*, 16 J. Marshall J. Computer & Info. L. 393, 399 (1998). However, as Professor Gomulkiewicz notes, the implied warranty of merchantability can be reframed to apply to software agreements. *Id.* at 400–02 (describing a proposal for application of an implied warranty of merchantability and quality of a computer program).

315. See, e.g., John A. Rothchild, *The Incredible Shrinking First-Sale Rule: Are Software Resale Limits Lawful?* 57 RUTGERS L. REV. 1, 25 (2004) (“It is very common for a license agreement accompanying the transfer of a software product to state that the software is ‘licensed’ to the end user, who is invariably referred to as the ‘licensee’ and never as the ‘purchaser’ of the software.”).

from an IOT device fails to secure the device and the associated data.

Many IOT devices lack anti-malware protection and have either no passwords or weak factory-set passwords, such as “admin,” “12345,” or “password,” which can easily be guessed by hackers.³¹⁶ IOT security failures may impact not only buyers, sellers and service providers but also unrelated third parties who become victims of distributed denial of service attacks where vulnerable IOT devices are weaponized by hackers.

Once a court determines under the functionality approach that a transaction is subject to Article 2, the following factors could be used to assess whether a company has adopted effective measures to enable a device to be fit for its ordinary purpose: (a) compliance with federal and state regulation or guidance on the IOT and data security and privacy issues, and industry wide initiatives,³¹⁷ (b) the adoption and implementation of detailed cybersecurity plans for dealing with data breaches, (c) the extent to which the company tests its systems, software programs, services, and devices for intrusion and weaknesses

316. David E. Sanger & Nicole Perlroth, *A New Era of Internet Attacks Powered by Everyday Devices*, N.Y. TIMES (Oct. 22, 2016), http://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html?_r=1 (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review).

317. For example, the U.S. Department of Commerce National Institute of Standards and Technology has recently issued security guidelines and engineering principles, and an introduction to the concepts of privacy engineering and risk management. RON ROSS, MICHAEL McEVILLEY & JANET CARRIER OREN, SYSTEMS SECURITY ENGINEERING, NIST SPECIAL PUBLICATION 800-160 (Nov. 2016), <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf>; SEAN BROOKS, MICHAEL GARCIA, NAOMI LEFKOVITZ, SUZANNE LIGHTMAN & ELLEN NADEAU, AN INTRODUCTION TO PRIVACY ENGINEERING AND RISK MANAGEMENT IN FEDERAL SYSTEMS, NISTR PUBLICATION 8062 (Jan. 2017), <http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>; *see also* Data Breach Insurance Act, H.R. 6032, 114th Cong. (2016) (proposing a bill that would give a fifteen percent tax credit to companies who purchase data breach insurance coverage and adopt the National Institute of Standard and Technology’s voluntary cybersecurity framework). In the financial services industry, states such as New York have proposed strong measures to force companies to protect consumer data. *See* New York State Department of Financial Services, Proposed Regulation, 23 NYCRR 500 (proposed Sept. 13, 2016), <http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf> (commenting on the need to establish certain regulatory minimum standards aimed at combatting cybersecurity issues in the financial services industry).

prior to making the product available to the public, (d) whether the company's IOT products are accompanied by anti-virus, anti-spyware and anti-malware software programs, (e) whether the company undergoes annual reviews and frequent penetration testing to assess the efficacy of cybersecurity measures after the product has been placed on the market, (f) whether the company timely and effectively addresses known security vulnerabilities, and (g) the extent to which a company monitors third party vendors or service providers that the company uses to handle customer data or systems connected to IOT devices.

Of course, in some instances, it may be unclear whether security flaws or vulnerabilities are due to the manufacturer's actions, an unrelated third party, or the device owner's failure to effectively use the security measures offered by the company. Additionally, since many IOT devices require access to a Wi-Fi network, internet service providers must play a crucial role in ensuring network security.

Further, courts should not ignore the impact of security fatigue—a phenomenon where consumers become “tired of being overwhelmed by the need to be constantly on alert, tired of all the measures they are asked to adopt to keep themselves safe, and tired of trying to understand the ins and outs of online security . . . which causes a sense of resignation and a loss of control.”³¹⁸ Security fatigue in the IOT setting may affect the choices and decisions of consumers, and companies should be primarily responsible for ensuring that IOT devices and all associated data are secure.

Because IOT devices may become vulnerable over time—where a manufacturer fails to provide the necessary software

318. Belton Zeigler, *The Next Threat to Cybersecurity: Consumer Fatigue*, LAW360 (Nov. 9 2016), <https://www.law360.com/articles/861219/the-next-threat-to-cybersecurity-consumer-fatigue> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review). See generally Brian Stanton, Mary F. Theofanos, Sandra Prettyman & Susanne Furman, *Security Fatigue*, IT PROFESSIONALS, Sept.–Oct. 2016, at 26 <https://www.computer.org/csdl/mags/it/2016/05/mit2016050026-abs.html> (last visited Mar. 5, 2017) (discussing a study conducted by the National Institute of Standards and Technology, which describes the impact of security fatigue on the online security experience of consumers) (on file with the Washington and Lee Law Review).

upgrades or fails to protect consumer data after delivery of the goods—the condition of the goods both prior to and after delivery should be considered.³¹⁹ The official comments to UCC section 2-314 suggest that there is room in the code for the evolution of new standards for assessing the implied warranty of merchantability.³²⁰

Consumers may also suffer intangible harms from privacy intrusions. One such example includes an FTC settlement order involving Aarons, a rent-to-own company, that permitted its franchisees to install software on rent-to-own products that allowed them to secretly track consumer locations and capture images of customer login information for financial and social media websites.³²¹ The sale of a device that contains software that is surreptitiously installed to obtain information about consumers and access to a customer's user accounts is not fit for its ordinary purpose and should give rise to a breach of implied warranty claim.

319. See, e.g., *Powers v. Am. Honda Motor Co.*, 79 P.3d 154, 157 (Idaho 2003) (noting that breach of the warranty of merchantability focuses on whether the goods are unmerchantable at the time of delivery); see also Timothy Davis, *UCC Breach of Warranty and Contract Claims: Clarifying the Distinction*, 61 BAYLOR L. REV. 783, 787 n.13 (2009) (contending that the warranty of merchantability does not extend to the future performance of delivered goods).

320. See U.C.C. § 2-314 cmt. 6 (AM. LAW INST. & UNIF. LAW COMM'N 2002) (stating that “[t]he language used is ‘must be at least such as . . .,’ and the intention is to leave open other possible attributes of merchantability”). Scholars have also proposed reforming tort law to address cybercrime. See, e.g., Michael L. Rustad & Thomas H. Keonig, *The Tort of Negligent Enablement of CyberCrime*, 20 BERKELEY TECH. L.J. 1553, 1558–59 (2005) (calling for the creation of a new tort of negligent enablement of cybercrime because of the failure of contract law to provide adequate protection to consumers).

321. See Allison Grande, *FTC Heads Face Senate Security Over Data Security Approach*, LAW360 (Sept. 27, 2016, 9:42 PM), <http://www.law360.com/articles/844593/ftc-heads-face-senate-scrutiny-over-data-security-approach> (last visited Mar. 5, 2017) (reporting on criticisms of the FTC's decision to continue pressing data security claims in cases where no consumers suffer no financial harm) (on file with the Washington and Lee Law Review); Linda Chiem, *FTC OKs Settlement In Rent-To-Own Co. Software Spying Row*, LAW360 (Mar. 11, 2014, 6:55 PM), <http://www.law360.com/articles/517559/ftc-oks-settlement-in-rent-to-own-co-software-spying-row> (last visited Mar. 5, 2017) (summarizing the Aaron's settlement agreement) (on file with the Washington and Lee Law Review).

If, at the time of contracting, the manufacturer or retailer knows of the particular purpose for which a buyer intends to use an IOT device—for instance, where the buyer has expressed a need for a secure device and related services and software that will be used for a specific objective—and the buyer relies on the seller’s expertise and knowledge in selecting the device, the buyer should have a cause of action for breach of the implied warranty of fitness for a particular purpose if the IOT device is insecure.³²²

Where an owner of an IOT device must use software and services provided in connection with the device for the device to operate and the owner has no choice but to permit the device to collect information about the owner, there is a reasonable expectation that the party collecting and storing this data will implement effective security measures to ensure that the device and data is secure. If the manufacturer or retailer fails to provide adequate security measures, owners of IOT devices should have a cause of action for breach of implied warranties under Article 2.³²³ Companies should not be permitted to

322. See U.C.C. § 2-315 (AM. LAW INST. & UNIF. LAW COMM’N 2002) (“Where the seller at the time of contracting has reason to know any particular purpose for which the goods are required and that the buyer is relying on the seller’s skill or judgment to select or furnish suitable goods, there is unless excluded or modified under the next section an implied warranty that the goods shall be fit for such purpose.”).

323. Even where Article 2 applies to a transaction, thereby implicating the implied warranties, consumers may still face additional hurdles in data breach lawsuits. Under Article 2, for example, a buyer’s failure to give notice to a seller may be fatal to the buyer’s cause of action. *Id.* § 2-607(3)(a). Additionally, in some cases, the standing requirement poses a significant problem for consumers in data breach lawsuits. See, e.g., *In re Zappos.com Inc.*, 108 F. Supp. 3d 949 (D. Nev. 2015). For example, the district court in *In re Zappos.com Inc.* found that the plaintiffs lacked standing in a data breach lawsuit because “[e]ven if Plaintiffs’ risk of identity theft and fraud was substantial and immediate in 2012, the passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something.” *Id.* at 958. However, in *Remijas v. Neiman Marcus Group*, the Seventh Circuit stated that the risk of identity theft or credit card fraud was immediate and real, reasoning that “Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing . . .” 794 F.3d 688, 693 (7th Cir. 2015); see also *Spokeo, Inc., v. Robins*, 136 S. Ct. 1540, 1549 (2016) (finding that to have standing a party must show, among other things, injury in fact that is concrete and particularized but concrete is not necessarily synonymous with

disclaim their liability for third party hacking and data leaks in the consumer context.

One could contend that, given the frequency with which hacking occurs, purchasers of IOT devices cannot have a reasonable expectation that the devices can be made completely free from vulnerabilities.³²⁴ In fact, the privacy policy of at least one IOT company specifically provides for the express assumption of risk by the consumer where there is an unauthorized access of their data by third parties.³²⁵ Nest's EULA provides that the company makes no warranties as to the security of the software provided in connection with their

tangible injuries and “intangible injuries can nevertheless be concrete”); *Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 WL 4728027 (6th Cir. Sept. 12, 2016) (applying *Spokeo* to hold that victims of data breach can sue without having to wait for their information to be misused). Moreover, even in distributed denial of service attacks, consumers may be able to meet standing requirements if they can prove that their device failed to work properly, such as where service or connection was interrupted because of the hack. Allison Grande, *Web Attack Piles Onto Internet of Things Security Concerns*, Law360 (Oct. 25, 2016), <https://www.law360.com/articles/854891/web-attack-piles-onto-internet-of-things-security-concerns> (last visited Mar. 5, 2017) (on file with the Washington and Lee Law Review). Additionally, where a company that manufactures an IOT medical device obtains FDA approval for the manufacture and sale of the device, and continues to comply with FDA standards, consumer claims—including breach of implied warranty claims—related to a defect in such a device may be prohibited. See *Riegel v. Medtronic, Inc.*, 552 U.S. 312, 329–30 (2008) (holding that the preemption clause of the Medical Device Amendments Act bars common law claims challenging the safety or effectiveness of a medical device marketed in a form that received premarket approval from the Federal Drug Administration and stating that “state requirements are pre-empted under the [Medical Device Amendments Act] only to the extent that they are ‘different from, or in addition to’ requirements imposed by federal law”).

324. See *Scenario ONE The New Normal*, CTR. FOR LONG-TERM CYBERSECURITY, U.C. BERKELEY, <https://cltc.berkeley.edu/scenario/scenario-one/> (last visited Mar. 5, 2017) (noting that by 2020 internet users may assume that their data will be stolen and broadcast) (on file with the Washington and Lee Law Review).

325. See, e.g., *Privacy Policy*, FiLIP (last updated Oct. 2014), <http://www.myfilip.com/privacy-policy/> (last visited Mar. 5, 2017) (“[W]e cannot guarantee that your personal information will be completely free from unauthorized access by third parties, such when transferred over or through systems not within our exclusive control. Your use of our FiLIP Service demonstrates your assumption of this risk.”) (on file with the Washington and Lee Law Review).

products.³²⁶ However, courts should be wary of permitting IOT companies to escape liability in data breach lawsuits based on this rationale. The data generated by IOT devices is extremely valuable to companies.³²⁷ As I have argued elsewhere, data analytics using aggregated IOT data sets can forecast the behaviors and preferences of customers.³²⁸ IOT companies must bear some responsibility for device failures and security issues, particularly where consumer data becomes vulnerable.

Some jurisdictions prohibit the disclaimer of implied warranties in consumer transactions.³²⁹ To the extent that a state does not prohibit the disclaimer of implied warranties in contracts involving merchants and consumers, these warranties should be made non-disclaimable in such transactions.³³⁰ These changes may be necessary given the various ways in which the impact of the Warranty Act has been limited as discussed in Part III.B above. Additionally, in at least one state that attempts to

326. See *End User License Agreement*, NEST, *supra* note 78 (“NEST LABS PROVIDES THE PRODUCT SOFTWARE ‘AS-IS’ AND DISCLAIMS ALL WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, QUIET ENJOYMENT, ACCURACY, AND NON-INFRINGEMENT OF THIRD-PARTY RIGHTS.”).

327. See Maverick, *supra* note 280 (providing statistics on the rapid growth of IOT data).

328. See Elvy, *supra* note 19, at 896 (“Amazon has obtained a patent for an anticipatory package shipping system that will analyze and predict consumer habits and deliver goods to consumers before they place an order.”).

329. See 3A LAWRENCE ANDERSON, UNIFORM COMMERCIAL CODE § 2-316:71 (3d ed. 2014) (listing jurisdictions).

330. The 2003 proposed revisions to Article 2 would have imposed specific language requirements for the disclaimer of implied warranties in consumer transactions, but under these revisions, such warranties would remain disclaimable as long as the disclosure requirements were satisfied. Revised Article 2, U.C.C. § 2-316(2) (AM. LAW INST. & UNIF. LAW COMM’N 2003) (Withdrawn 2011). In addition to state prohibitions on the disclaimer of implied warranties, a few states have taken an aggressive approach to addressing the warranty problem in consumer transactions by adopting separate statutes aimed at preventing consumers from being deceived into believing that contract provisions, which violate their rights under existing law are valid. See The New Jersey Truth-In-Consumer Contract Warranty and Notice Act *N.J.S.A.* 56:12–15. The act establishes liability when a contract or other writing by a “seller, lessor, creditor, lender or bailee” violates a consumer’s established legal right. *Id.*; see also Sponsors’ Statement, *Statement to Assembly Bill No. 1660* (May 1, 1980).

limit the effect of warranty disclaimers, this restriction appears to extend only to personal injury claims.³³¹ As such, in the IOT context, the adoption of new disclaimer prohibitions should extend to both personal injury as well as economic loss. In some states, privity requirements may also need to be relaxed to avoid vertical privity issues and to permit actions by third party non-purchasers who suffer economic rather than personal injury harms.³³² The application of Article 2 to IOT transactions and the widespread prohibition of implied warranty disclaimers in consumer transactions could encourage IOT companies to keep IOT devices and consumer data secure.

One could contend that prohibiting warranty disclaimers and extending implied warranties to the software and services aspect of a hybrid consumer transaction could lead to increased costs for companies which are ultimately passed on to consumers. Of course, this assumes to some extent that the use of warranty disclaimers in form contracts lowers costs for companies and that these companies pass along these savings to consumers. As with other form contract provisions, such as arbitration clauses, it is likely challenging to assess whether the inclusion of warranty disclaimers in consumer contracts generate cost savings for companies. Further, as the Consumer Financial Protection Bureau has noted “whether such savings, to the extent they exist, are passed along to consumers is even more difficult to establish or disprove.”³³³ Concerns about

331. See ALA. CODE §§ 7-2-316(5), 7-2-719(4) (1975) (stating that nothing in the disclaimer provisions “shall be construed so as to limit or exclude the seller’s liability for damages for injury to the person in the case of consumer goods”).

332. See U.C.C. § 2-318 (AM. LAW INST. & UNIF. LAW COMM’N 2002) (describing three alternatives for third party beneficiaries of warranties); see also JAMES J. WHITE & ROBERT S. SUMMERS, UNIFORM COMMERCIAL CODE § 12-3, 546 (2017) (noting that third party non-purchasers must allege personal injury in most states under Article 2).

333. CONSUMER FIN. PROT. BUREAU, ARBITRATION STUDY: REPORT TO CONGRESS, PURSUANT TO DODD-FRANK WALL STREET REFORM AND CONSUMER PROTECTION ACT § 1028(a), § 10.3, at 15 (2015) [hereinafter “CFPB Study”]; see also *CFPB Study Finds That Arbitration Agreements Limit Relief for Consumers*, Consumer Fin. Prot. Bureau (Mar. 20, 2015), <http://www.consumerfinance.gov/about-us/newsroom/cfpb-study-finds-that-arbitration-agreements-limit-relief-for-consumers/> (last visited Mar. 5, 2017) (noting that based on the CFPB study “there is no evidence of arbitration clauses leading to lower prices for consumers”)

potential increases in the price of IOT products due to the imposition of non-disclaimable implied warranties in hybrid IOT consumer contracts are likely outweighed by the serious privacy and cybersecurity issues posed by the IOT, and the growing need to encourage companies to effectively address security issues.

Another possible objection to the application of implied warranties under a functionality approach is that a private ordering solution will effectively protect consumers. For example, companies in various industries, including businesses in the retail, health and financial services sectors, have initiated bug bounty programs that pay up to \$200,000 and provide other benefits for information on security weaknesses.³³⁴ These programs are intended to encourage security researchers to inform companies of security vulnerabilities.³³⁵ Since 2013, there has been a large increase in the number of companies that have adopted these programs.³³⁶ Despite the adoption of such a program, a company may obtain information about security vulnerabilities but may not always effectively act to remedy the issue or disclose the problem to customers. Such programs are also not designed to compensate consumers for harms suffered as a result of security flaws. Additionally, companies continue to disclaim implied warranties and may exclude from express warranties software and services needed to operate IOT devices.

Article 2's role in data breach suits becomes increasingly important in light of the potential limitations of tort law. For example, in a data breach case, the Third Circuit held that the plaintiffs' negligence claims were barred under the economic loss doctrine, which provides that "no cause of action exists for

(on file with the Washington and Lee Law Review).

334. See Kim Perretti, *You Don't Need A Data Breach To Face Regulatory Scrutiny*, LAW360 (Sept. 26, 2016, 9:29 AM), <http://www.law360.com/articles/842172/you-don-t-need-a-data-breach-to-face-regulatory-scrutiny> (last visited Mar. 5, 2017) (commenting on the increase in regulatory and litigations actions based on identified security vulnerabilities, rather than breaches) (on file with the Washington and Lee Law Review).

335. See *id.* ("Bug bounty programs (also referred to as vulnerability disclosure programs) provide incentives, such as cash, airline miles or just recognition to security researchers who report vulnerabilities to companies.").

336. See *id.* (reporting that the number of companies with these programs has tripled since 2013).

negligence that results solely in economic damages unaccompanied by physical or property damage.”³³⁷ Courts in Pennsylvania, Georgia, Illinois and Massachusetts have all dismissed data breach suits under the economic loss doctrine.³³⁸

In *In re Sony Gaming*, a consumer data breach lawsuit, the court held that the economic loss doctrine barred the plaintiffs from recovering economic damages, including the cost “to purchase credit monitoring services,” “loss of use and value of Sony Online Services,” “loss of use and value of Third Party Services,” and “a diminution in value of Plaintiffs’ Consoles.”³³⁹ To the extent that the economic loss doctrine applies, consumers may be prohibited from recovering purely economic losses under a negligence theory.³⁴⁰ This highlights the importance of the application of Article 2 to IOT transactions.

337. *Sovereign Bank v. BJ’s Wholesale Club, Inc.*, 533 F.3d 162, 176 (3d Cir. 2008) (internal citations omitted). In applying the economic loss doctrine the court stated “to allow a cause of action for negligent cause of purely economic loss would be to open the door to every person or business to bring a cause of action. Such an outstanding burden is clearly inappropriate and a danger to our economic system.” *Id.*

338. *See In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1171 (D. Minn. 2014) (stating that courts in California, Georgia, Illinois, Massachusetts, and Pennsylvania have faced data-breach claims and all of these courts dismissed the negligence claims based on the economic loss rule); *see also In re TJX Companies Retail Sec. Breach Litig.*, 564 F.3d 489, 498–99 (1st Cir. 2009), as amended on reh’g in part (May 5, 2009) (holding that a bank’s negligence claims were barred by the economic loss doctrine); *Sovereign Bank*, 533 F.3d at 175–78 (same); *Willingham v. Glob. Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *17–19 (N.D. Ga. Feb. 5, 2013) (dismissing negligence claims with prejudice based on the economic loss doctrine); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528–30 (N.D. Ill. 2011) (noting that the economic loss rule can apply to product liability and negligence claims).

339. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 965 (S.D. Cal. 2014) (holding that an everyday consumer transaction does not constitute a special relationships for purposes of the economic loss doctrine).

340. In some jurisdictions the impact of the economic loss doctrine can be avoided where there is special relationship between the parties or where unique circumstances justify risk allocation. *See, e.g., Aardema v. U.S. Dairy Sys., Inc.*, 215 P.3d 505, 512 (Idaho 2009) (noting that a special relationship only exists in two situations: “(1) ‘where a professional or quasi-professional performs personal services [:]’ and (2) ‘where an entity holds itself out to the public as having expertise regarding a specialized function, and by so doing, knowingly induces reliance on its performance of that function.’” (citations omitted)). Factors to

C. Article 9's Embedded Approach

Given that software is now routinely embedded within devices, Article 9's definition of goods may be particularly useful for the IOT era. First, Article 9 of the UCC excludes from the definition of goods software embedded in goods that consist "solely of the medium in which the program is embedded."³⁴¹ If the software is offered on a computer disc or where the software retains its independent status apart from the goods, it would likely be viewed as a general intangible rather than a good under Article 9.³⁴² As discussed in Part III above, IOT devices are distinct from software transactions involving computer discs.³⁴³

Second, under Article 9, goods are defined to include software embedded within goods and supporting information provided in connection with the transaction if the software is customarily considered as part of the goods or if by owning the goods a person acquires a right to use the software associated with the goods.³⁴⁴ Under this definition, an IOT device could be considered a good even though the device contains embedded software because a purchaser of an IOT device obtains a license

consider in evaluating the parties' relationship include:

- (1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct and (6) the policy of preventing future harm.

J'Aire Corp. v. Gregory, 598 P.2d 60, 63 (Cal. 1979).

341. U.C.C. § 9-102(a)(44) (AM. LAW INST. & UNIF. LAW COMM'N 2010).

342. *See id.* § 9-102(a)(76) (defining software as a computer program and any supporting information provided in connection with a transaction relating to the program and noting that the term does not include a computer program that is included in the definition of goods); *id.* at § 9-102(a)(42) (describing software as a general intangible); *see also* Steven O. Weise, *The Financing of Intellectual Property Under Revised UCC Article 9*, 74 CHI. KENT L. REV. 1077, 1086 (1999) (contending that where software retains its independent status it is a general intangible); Towle *supra* note 227, at 547 (contending that Article 9 expressly provides that a computer program does not become a good simply because it is embedded on a tangible medium—a disc).

343. *Supra* Part III.

344. U.C.C. § 9-102(a)(44) (AM. LAW INST. & UNIF. LAW COMM'N 2010).

to use the services and software provided by the manufacturer or retailer.

Ultimately, buyers of IOT devices expect software to be provided in connection with devices to allow the devices to perform the functions advertised by manufacturers, thereby making it customary that such programs are considered to be part of IOT devices.³⁴⁵ Thus, “[w]hen software is embedded and marketed as an integral part of goods, many, if not most, people would consider the software to be part of the goods.”³⁴⁶

Article 9’s definition of goods is similar to the approach contained in previous proposed revisions to Article 2 (“Revised Article 2”), which were ultimately withdrawn.³⁴⁷ The definition of goods in Revised Article 2 excluded information not associated with goods but it is unclear whether the term information was intended to cover software.³⁴⁸ The comments to Revised Article 2 suggested that the sale of “smart goods,” such as an automobile with computer programs, is likely a transaction in goods subject

345. See Brenan, *supra* note 203, at 427 (contending that Article 9’s free transferability policy severely restricts a licensor’s ability to prevent a forced dedication of its royalties to a licensee’s secured lender and the Copyright Act has long addressed “embedded software” in express statutory provisions and so there was no need for Article 9 to do so).

346. SOFTWARE PRINCIPLES, *supra* note 44, § 1–2; see also *American Bar Association Working Group Report on the Uniform Computer Information Transactions Act*, AM. BAR. ASSOC. (Jan. 31, 2002), <http://www.americanbar.org/content/dam/aba/migrated/leadership/ucita.authcheckdam.pdf> (suggesting that how goods containing software are marketed should be a relevant factor in assessing whether UCITA should govern a transaction). The functionality approach described in this Article considers not only the role of software in goods but also the novel IOT services described herein that are equally as central to the functionality of IOT devices. However, not all intellectual property scholars agree with this line of reasoning. See Brenan, *supra* note 345 and accompanying text (suggesting that a computer program could never be associated with the goods in such a manner that it customarily is considered part of the goods because the Copyright Act specifically negates this result).

347. Revised Article 2, U.C.C. § 2-103(k), cmt. 7 (AM. LAW INST. & UNIF. LAW COMM’N 2003) (Withdrawn 2011).

348. *Id.* Additionally, states such as Oklahoma have specifically excluded information from Article 2’s definition of goods. OKLA. STAT. ANN. tit. 12A, § 2-105(1) cmt. 1 (West 2016); see also Kim, *The Software Licensing Dilemma*, *supra* note 198, at 1110 (contending that Revised Article 2 “added ‘information’ to the list of things that are *not* considered goods, but left unresolved whether software products are ‘goods’ or ‘information.’” (emphasis added)).

to Article 2.³⁴⁹ However, Revised Article 2 stopped short of definitively bringing such transactions within the scope of Article 2.

The proposed comments did not address whether software subsequently downloaded to smart products would be excluded from Article 2 because the transfer was electronic.³⁵⁰ The comments to Revised Article 2 went on to provide that whether a hybrid transaction involving the sale of goods and software falls within the scope of Article 2 is a determination to be made by courts and a court may elect to apply Article 2 to only the goods aspect of the transaction.³⁵¹ This approach would have authorized courts to use the predominant purpose and gravamen of the claim tests to assess hybrid transactions, both of which are problematic.

In contrast, Article 9 more succinctly addresses the issue of computer programs embedded within goods.³⁵² Article 9's application to security interests involving goods embedded with software does not prevent the application of federal intellectual property law, but Article 9 will not apply to the extent that it is preempted. In fact, the revisions to amended Article 9 were intended to "facilitate the ability of a licensee of intellectual property to obtain financing secured by its rights under the license."³⁵³

Currently, Article 2 relies only on Article 9's definition of consumer goods.³⁵⁴ The definition of goods would be more

349. *Id.*

350. Braucher, *supra* note 34, at 269–71. The proposed comments did suggest that the transaction in the *Specht* case would not be subject to Article 2. *See generally* Revised Article 2, U.C.C. § 2-103(k), cmt. 7 (AM. LAW INST. & UNIF. LAW COMM'N 2003) (Withdrawn 2011).

351. *See generally* Revised Article 2, U.C.C. § 2-103(k), cmt. 7 (AM. LAW INST. & UNIF. LAW COMM'N 2003) (Withdrawn 2011).

352. *See* 1-11 SOFTWARE LICENSING § 11.05 (2015) (noting that chips controlling a car's brakes, security system, heating system's thermostat, or a Mr. Coffee machine are classified as goods under Article 9). *See generally* Edwin E. Smith, *A Summary of the Provisions of Article 9 of the Uniform Commercial Code, Asset Based Financing 2009*, in PRACTICING LAW INSTITUTE, COMMERCIAL LAW AND PRACTICE COURSE HANDBOOK SERIES 707 (2009).

353. Weise, *supra* note 342, at 1092.

354. U.C.C. § 2-103(3) (AM. LAW INST. & UNIF. LAW COMM'N 2001) (noting that

consistent across the different articles of the UCC if Article 2 were amended to adopt the provisions of Article 9's definition of goods that relate to computer programs.

One potential drawback to the Article 9 approach is that it fails to account for the different services that may be provided by companies in connection with IOT devices. This could then mean that Article 2 would apply to the sale of the device with the embedded software and perhaps the associated software updates, but not necessarily the services provided by the company that also allows the device to operate. A functionality test or a products approach to Article 2 may be advantageous for this reason.

Another objection to using the Article 9 embedded approach is that eventually it may become difficult to differentiate between embedded and non-embedded software.³⁵⁵ Such an attempted differentiation also begs the question of whether pre-embedded software should be viewed differently from downloaded software, both of which may be necessary for IOT devices to continue to operate as intended.

Manufacturers may eventually design IOT devices in such a manner that the software is no longer within the device but provided through other means, such as cloud computing, for example. Thus, even if Article 2 were amended to clearly extend to goods embedded with software, goods associated with non-embedded software may not fall within Article 2's scope. Of course, Article 9's definition of goods includes not only a computer program embedded in goods but also "supporting information provided in connection with a transaction relating to the program."³⁵⁶ To the extent that software updates and non-embedded software could be viewed as "supporting information," one could contend that these types of software—that are related to goods—and computer programs—embedded within the goods—fall within the definition of goods.

the definition of consumer goods in section 9-102 applies to Article 2).

355. Braucher, *supra* note 34, at 250; *see also* Philp Koopman & Cem Kaner, *The Problem of Embedded Software in UCITA and Drafts of Revised Article 2*, 43 U.C.C. BULL., rel. 1 & 2 (2001).

356. U.C.C. § 9-102(a)(44) (AM. LAW INST. & UNIF. LAW COMM'N 2010).

Under the functionality approach, the medium through which the software is provided does not determine whether Article 2 would apply to a transaction. Under the functionality test, where the software is central to the operations of the device, Article 2 could apply to the transaction regardless of whether the software is pre-loaded onto the device, subsequently downloaded onto the device or provided via cloud computing.

D. Exclusionary Approach

Another potential solution to the issues posed by hybrid transactions is to amend Article 2 to exclude software embedded in goods and all transactions involving a combination of goods, software and services.³⁵⁷ Such an approach would certainly improve predictability and clarity in this area because parties would know prior to contracting that, where goods are associated with software or services and are provided together, the transaction would not be subject to Article 2. Justification for this approach could be found in section 2-102, which provides that Article 2 applies to transactions in goods.³⁵⁸

One could argue that Article 2 was intended to cover transactions in goods only and not transactions involving software or services. To some extent the predominant purpose and the gravamen of the claim tests reflect this point because under these tests, Article 2 applies only where the main purpose of the transaction is for the sale of goods or where a party's claim is related to the goods that were provided. These tests focus on separating the goods aspect of the transaction from the services or software portion of the agreement.

357. In proposed amendments to Article 2, information was excluded from the definition of goods and the National Conference of Commissioners on Uniform States Law had proposed but later failed to approve a definition of information which would have defined information as "data, text, images, sounds, mask works, computer programs, software, databases, or the like, including collections and compilations. The term includes computer information." National Conference of Commissioners on Uniform State Laws, *Proposed Amendments to Uniform Commercial Code Article 2—Sales* (2002), http://www.uniformlaws.org/shared/docs/ucc2and2a/ucc2_am02.pdf; see also Lee Kissman, Comment, *Revised Article 2 and Mixed Goods/Information Transactions: Implications for Courts*, 44 SANTA CLARA L. REV. 561, 566 (2004).

358. U.C.C. § 2-102 (AM. LAW INST. & UNIF. LAW COMM'N 2002).

However, this is an overly restrictive interpretation of section 2-102. IOT devices satisfy the definition of goods because they are movable items and, in this manner, are arguably no different from the goods of the pre-information era, with the exception of the software and services accompanying the devices. Section 2-102 does not provide that Article 2 applies “only to transactions in goods” or “only to transactions involving the sale of goods” rather it states that Article 2 applies to “transactions in goods.” This suggests that Article 2’s scope can and should extend to all agreements involving goods even where software and services are involved in the transaction and even though there may be other provisions of Article 2 which arguably apply only to contracts for the sale of goods.

Additionally, even though the predominant purpose and the gravamen of the claim tests attempt to focus on the goods aspect of a transaction, courts have long recognized that it is possible for Article 2 to apply to transactions that involve not only goods but services as well. As such, excluding IOT hybrid transactions from the scope of Article 2 would contradict the express language of section 2-102.

A products approach, functionality approach or Article 9 approach to this problem recognizes the potential breadth of section 2-102. Under these three approaches Article 2 could possibly apply to transactions involving the sale of goods even where such a transaction also involves the provision of services or software. Further, if an exclusionary approach were adopted, Article 2 breach of implied warranty claims may be rendered obsolete in data breach and hacking cases involving IOT devices.

V. Conclusion

The IOT is expected to generate “self-sustaining autonomous systems,”³⁵⁹ and where necessary, existing legal frameworks must evolve in the face of this new reality. While there are certainly areas of Article 2 that can be improved, it remains the best source of unified state law available to evaluate IOT transactions. However, given Article 2’s ambiguity on the

359. Choudhary, *supra* note 237, at 239.

issue of hybrid transactions and the fact that it is questionable whether there will be widespread application of common-law service warranties, UCITA and the Software Principles, there is a strong need to increase uniformity and clarity in this area.

IOT transactions involve an intricate provision of connected hardware, services and software in which software and services constitute an integral, if not the predominant, part of the transaction. In the IOT era, the functionality of goods depends on software and services. As a result, the purchaser's relationship with a manufacturer or retailer must continue well beyond the initial sale of the device. In this way, hybrid IOT transactions are distinct from the hybrid transactions of old.

The cost of sensors, embedded processors and cloud computing has decreased dramatically resulting in large numbers of IOT devices that can be easily manufactured by companies.³⁶⁰ As a result, "literally everything will have IOT technology at some point."³⁶¹ Even if one does not believe that IOT hybrid transactions will be fundamentally different from other types of transactions—including software transactions—the expected proliferation of software-dominated and connected IOT devices, and the lack of explicit clarity in Article 2 on how to deal with hybrid transactions, combined with the well-documented inadequacies of the predominant purpose test justify calls for the development of new frameworks in this area or, at the very least, discourse about Article 2's role in the IOT setting. Resolving the long-standing ambiguity regarding Article 2's applicability to hybrid transactions promotes uniformity of the "laws of various jurisdictions," which is a central and important goal of the UCC.³⁶²

This Article proposed and evaluated four potential solutions for addressing hybrid IOT transactions with the aim of improving clarity, simplicity and uniformity. Ultimately, a functionality approach may be the preferred method for evaluating IOT hybrid transactions because this test accounts

360. Paul Taylor, *How The Internet Of Things Makes Dumb Devices Smart*, FORBES, <http://www.forbes.com/sites/sap/2016/09/22/how-the-internet-of-things-makes-dumb-devices-smart/#38cae0f7726c> (last visited Mar. 5, 2017) (describing advancements in IOT devices) (on file with the Washington and Lee Law Review).

361. *Id.*

362. U.C.C. § 1-103(a)(3) (AM. LAW INST. & UNIF. LAW COMM'N 2002).

for the uniqueness of IOT hybrid transactions where a device's operations are contingent upon the provision of software and services.

The functionality solution avoids the time-consuming process needed to amend the UCC, which would be required for the implementation of the products approach, the Article 9 embedded approach and the exclusionary approach. Courts could simply begin applying the functionality test to IOT hybrid transactions in place of the predominant purpose test. Of course, amendments may be needed to more effectively prohibit disclaimers of implied warranties in consumer transactions.

The functionality approach represents a compromise between the all or nothing approach of the products and exclusionary solutions, which would either bring the entire transaction under Article 2's scope or exclude such transactions from Article 2 in all cases. Under the functionality test, transactions involving goods, software and services are subject to Article 2 only where the services and software are integral to the device's operations. In this way, the functionality test strikes an appropriate balance.

Section 1-103 of the UCC notes that modernization of the law of commercial transactions is an important policy underpinning the code and its provisions must be liberally construed.³⁶³ In keeping with these goals, the IOT will revolutionize the types of goods that are sold to buyers and the provisions of the UCC must be generously interpreted to account for this new era.

363. *Id.* § 1-103(a).