Harvard Journal of Law & Technology
Volume 37, Number 3 Symposium 2023

COMMERCIAL LAW AS A SOURCE OF PRIVACY AND CYBERSECURITY PROTECTION

*Stacy-Ann Elvy**

ABSTRACT

In 2022, the American Law Institute and the Uniform Law Commission approved important amendments to the Uniform Commercial Code ("UCC") to address various technological developments. This Essay explores the potential role of these revisions to the UCC and other related sources of law in helping to protect consumer privacy and security in the Internet of Things ("IoT") setting. IoT devices often rely on an ongoing provision of services and software from companies to function optimally. This ongoing relationship combined with the surveillance capabilities of many IoT devices allows device manufacturers, service providers, and other entities to collect a wealth of data about device users and others. The UCC has the capacity to play a central role in determinations regarding liability for privacy and cybersecurity invasions involving IoT devices and systems. I argue that the existing implied warranty of merchantability under the UCC could serve as an important privacy and cybersecurity enforcement mechanism.

* Professor of Law and Martin Luther King Jr. Hall Research Scholar, University of California, Davis School of Law (J.D., Harvard Law School, 2004; B.S., Cornell University, 2001). I am grateful to my research assistant Nicholas Takton and the student editors of the *Harvard Journal of Law & Technology* for their invaluable help.

TABLE OF CONTENTS

I. INTRODUCTION

Approximately seventeen billion Internet of Things ("IoT") objects are currently in use worldwide.[1] The IoT highlights ambiguities in and raises a host of legal questions and challenges to existing sources of commercial law, such as the Uniform Commercial Code ("UCC"). One such challenge is the potential application of the UCC to hybrid transactions involving goods, services, and software. Another related issue concerns the role of the UCC's implied warranty of merchantability in resolving modern disputes involving software and service-dependent objects that collect consumer data. In 2022, the American Law Institute ("ALI") and the Uniform Law Commission approved important amendments to the UCC ("2022 UCC Amendments") to address hybrid transactions and various technological developments, including digital assets.[2] This Essay explores the potential role of these amendments to Article 2 of the UCC ("Article 2") in helping to both promote fair dealing between consumers and merchants and protect consumers' reasonable expectations of privacy and cybersecurity.

IoT devices often rely on an ongoing provision of services and software to function optimally.[3] This ongoing relationship, combined with the surveillance capabilities of many IoT devices, raises several privacy and cybersecurity concerns. IoT devices allow traditionally mundane

---

1. Elizabeth MacBride, *The Dark Web's Criminal Minds See Internet of Things as Next Big Hacking Prize*, CNBC (Jan. 9, 2023, 9:29 AM), https://www.cnbc.com/2023/01/09/the-dark-webs-criminal-minds-see-iot-as-the-next-big-hacking-prize.html [https://perma.cc/2R6T-PYHC]; LOPEZ RSCH., AN INTRODUCTION TO THE INTERNET OF THINGS (IOT): PART 1 OF "THE IOT SERIES" 2 (2013), www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf [https://perma.cc/A3BM-ALBU] (describing the IoT and noting that the term was coined by Kevin Ashton).

2. *Legislative Bill Tracking*, AM. L. INST. & UNIF. L. COMM'N, https://www.uniformlaws.org/committees/community-home?communitykey=1457c422-ddb7-40b0-8c76-39a1991651ac [https://perma.cc/YQ5M-5RWN].

3. Michael Bosson, *Helpful Tips for Updating IoT Devices*, ONOMONDO (June 27, 2023), https://onomondo.com/blog/iot-device-update-tips [https://perma.cc/289H-YVUQ]; Sebastian Polly, *Over-the-Air Software Updates for IoT Devices Present Companies with Product Liability and Safety Opportunities — and Challenges*, HOGAN LOVELLS (May 22, 2018), https://www.hoganlovells.com/en/publications/over-the-air-software-updates-for-iot-devices [https://perma.cc/9LAW-XD8D].

offline activities, such as turning on a light or ringing a neighbor's doorbell, to be transformed into online activities. Once individuals' offline activities are converted into online activities and millions of data points about individuals are collected, the potential for data monetization and exploitation increases. Granular IoT data can be used to paint a detailed picture of individuals' behaviors, lives, and preferences.[4]

IoT devices and related systems are also susceptible to cyberattacks. Some IoT devices lack embedded security measures found in other products.[5] Unsecured wireless networks; employee and device user error; and mediocre data encryption methods, data storage, and transmission practices may all contribute to cybersecurity risks associated with IoT devices.[6] A lack of software updates may also prove detrimental.[7]

IoT device manufacturers' frequent integration of firmware in IoT devices, which relies excessively on third-party components ("TPCs") to simplify and speed up product development,[8] also contributes to cybersecurity risks.[9] A single IoT device could rely on multiple TPCs, and a single device manufacturer may incorporate the same TPCs across different IoT products, which allows a hacker familiar with a vulnerability common to a specific TPC to simultaneously attack multiple devices that rely on the same TPC.[10] One study evaluating 584 TPCs in firmware in IoT devices detected 128,757 security vulnerabilities and observed that

---

4. Heather Richter Lipford, Madiha Tabassum, Paritosh Bahirat, Yaxing Yao & Bart P. Knijnenburg, *Privacy and the Internet of Things*, *in* MODERN SOCIO-TECHNICAL PERSPECTIVES ON PRIVACY 233, 257 (Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes & Jennifer Romano eds., Springer 2022).

5. Bree Fowler, *How to Protect Your Child's Privacy on Internet-Connected Toys*, CONSUMER REPS. (Jan. 9, 2018), https://www.consumerreports.org/privacy/how-to-protect-child-privacy-on-internet-connected-toys-a1031039278 [https://perma.cc/TL94-AZAP].

6. STACY-ANN ELVY, A COMMERCIAL LAW OF PRIVACY AND SECURITY FOR THE INTERNET OF THINGS 59–80 (2021); Marie-Helen Maras, *4 Ways "Internet of Things" Toys Endanger Children*, SCI. AM. (May 10, 2018), https://www.scientificamerican.com/article/4-ways-internet-of-things-toys-endanger-children [https://perma.cc/8LFX-WDM7]; Christopher Mims, *Why Even Big Tech Companies Keep Getting Hacked — and What They Plan to Do About It*, WALL ST. J. (Sept. 24, 2022, 12:00 AM), https://www.wsj.com/articles/cyber attacks-hacking-lapsuss-zero-trust-okta-uber-rockstar-11663969967?st=ynbd07lmf4vpfkl [https://perma.cc/NZH9-KWVC].

7. Tatum Hunter, *Want to Avoid a Cyberattack? Stop Ignoring Those Pesky Software Updates.*, WASH. POST (Mar. 1, 2022), https://www.washingtonpost.com/technology/2022/02/24/software-update-security-cyberattack [https://perma.cc/8Z62-M3DY].

8. *See* Binbin Zhao, Shouling Ji, Xuhong Zhang, Yuan Tian, Qinying Wang, Yuwen Pu et al., *UVSCAN: Detecting Third-Party Component Usage Violations in IoT Firmware*, USENIX SEC. SYMP., June 2023, at 1, 1–2 (discussing "the security risks that can emerge if developers fail to double check the software specifications provided by TPCs, which contain software components of a reusable nature that can thereby shorten the product development cycle").

9. *See generally* BINBIN ZHAO, SHOULING JI, JIACHENG XU, YUAN TIAN, QIUYANG WEI & QINYING WANG ET AL., ONE BAD APPLE SPOILS THE BARREL: UNDERSTANDING THE SECURITY RISKS INTRODUCED BY THIRD PARTY COMPONENTS IN IOT FIRMWARE (2022), https://arxiv.org/pdf/2212.13716.pdf [https://perma.cc/S9LD-JMS8] ("TPCs are not secure, and the vulnerabilities in TPCs will influence the security of IoT firmware.").

10. *Id.* at 1, 8.

some vendors refrain from adopting new TPCs and continue to use older versions in product development, despite known vulnerabilities, to avoid issues associated with decreased performance and stability.[11]

Section 5 of the Federal Trade Commission Act ("FTCA") prohibits "unfair or deceptive acts or practices" impacting commerce.[12] This prohibition serves as the basis for many of the Federal Trade Commission's ("FTC's") privacy and cybersecurity enforcement activities, but the FTCA lacks a private right of action.[13] This Essay argues that the existing implied warranty of merchantability found in Article 2 could serve as an alternative source of privacy and data security protection and provide consumers with a private cause of action. Standards set forth in Article 2 for determining merchantability, such as whether a good is fit for its ordinary purpose[14] and whether a good conforms to certain promises and affirmations of fact,[15] could in some instances be used to address privacy and cybersecurity failures involving IoT devices and related services. This Essay also exposes potential hurdles to the effective use of the merchantability warranty and offers a path forward via a functional approach to hybrid transactions. There are potential benefits and drawbacks to new guidance on this issue provided in the 2022 UCC Amendments. Additional possible challenges to the use of the merchantability warranty in the IoT context include the frequent use of warranty disclaimers and questions about the duration and timing of the merchantability warranty.

II. THE HYBRID TRANSACTIONS PROBLEM

Article 2 of the UCC "applies to transactions in goods," but its core focus is the "sale of goods."[16] Historically, one of the most important unsettled issues under the code is how to determine when Article 2 applies to transactions that involve goods and non-goods. Under Article 2, the term "goods" is defined in part as "all things (including specially manufactured goods) which are movable."[17] I use the term non-goods to refer to offerings, such as software and services. The non-goods aspect of a transaction may not always consistently meet Article 2's

11. *Id.* at 13.

12. 15 U.S.C. § 45(a)(1) (2020).

13. CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 113 (2016); Pressley v. Exeter Fin. Corp., No. 21–3641, 2022 U.S. Dist. LEXIS 130972, at *7 (E.D. Pa. July 22, 2022).

14. U.C.C. § 2-314(2)(c) (AM. L. INST. & UNIF. L. COMM'N 1995).

15. *Id.* § 2-314(2)(f).

16. U.C.C. § 2-102 (AM. L. INST. & UNIF. L. COMM'N 2001); LINDA J. RUSCH & STEPHEN L. SEPINUCK, COMMERCIAL LAW: PROBLEMS AND MATERIALS ON SALES AND PAYMENTS 6 (West Academic 2d ed. 2012).

17. *Id.* § 2-105(1).

definition of a sale, which requires title to pass from seller to purchaser for a stated price.[18]

Article 2 provides buyers with a cause of action for non-disclaimed breach of implied warranties.[19] Historically, if a transaction was not subject to Article 2, then its accompanying warranties did not apply to the transaction unless similar warranties were located in another potentially applicable source of law or a court elected to apply the UCC's provisions by analogy.[20] IoT devices' deep connection to software, connected systems, and continuous services makes it even more difficult to determine when transactions involving goods and non-goods should be subject to Article 2. If courts widely find that such transactions fall outside of Article 2 or decline to apply Article 2 by analogy, then Article 2 could quickly become less influential, considering the speed at which companies currently manufacture IoT devices with significant connections to services and software.[21]

The goods of today's connected world are no longer the static physical objects that have dominated the consumer marketplace, and which, "once placed with an individual, belong[] to that person."[22] Unlike their predecessors, modern movable objects cannot easily be divorced from connected services and software.[23] For example, if an individual purchases a non-IoT household good and an installation service from the

---

18. *Id.* § 2-106(1).

19. U.C.C. §§ 2-316, 2-714(2) (AM. L. INST. & UNIF. L. COMM'N 2017).

20. Uniform Computer Information Transactions Act § 403, cmt. 1 (NAT'L CONF. OF COMM'RS ON UNIF. STATE L. 2002); Gary D. Spivey, Annotation, *Application of Warranty Provisions of Uniform Commercial Code to Bailments*, 48 A.L.R.3d 668 § 3–6 (1973) (discussing courts' application of Article 2 warranties to non-sales transactions and noting that "the warranty sections of Article 2 are not designed in any way to disturb those lines of case-law growth which have recognized that warranties need not be confined to sales contracts, but may arise in other appropriate circumstances"); Nancy Kim, *Beyond Section 230 Liability for Facebook*, 96 ST. JOHN'S L. REV. 353, 384 (2022) ("[C]ourts have often cited the UCC by analogy where goods are not involved."); Raymond T. Nimmer, *Through the Looking Glass: What Courts and UCITA Says About the Scope of Contract Law in the Information Age*, 38 DUQ. L. REV. 255, 264 (2000) (discussing cases in which courts apply Article 2's provisions to non-sales transactions by analogy).

21. *See, e.g.*, *In re* VTech Data Breach Litig., No. 15-CV-11620, 2017 U.S. Dist. LEXIS 103298, at *30–33 (N.D. Ill. 2017) (discussing physical toys that had online service features and finding that since the claim was "based on a defective service, not a good, the complaint fails to state a claim for breach of the implied warranty of merchantability"); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 954–59 (S.D. Cal. 2014) (discussing how the claims, which involved the PlayStation gaming console and its online networks, were possibly subject to dismissal under the UCC since "the implied warranty of merchantability . . . only applies to 'transactions in goods'").

22. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET — AND HOW TO STOP IT 106 (2008); Anupam Chander, *The Internet of Things: Both Goods and Services*, 18 WORLD TRADE REV. 9, 9–11 (2019).

23. *See generally* Stacy-Ann Elvy, *Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77 (2017) (discussing novel IoT products with such capacity and related legal issues); Aaron K. Perzanowski, Chris Jay Hoofnagle & Aniket Kesari, *The Tethered Economy*, 87 GEO. WASH. L. REV. 783 (2019) (citing *id.* at 82–86).

manufacturer, this traditional household good could continue to function without the manufacturer providing any ongoing services or software (with the possible exception of needed repairs once installed). Similarly, if a homeowner hires a business to supply and install new roof shingles, such a transaction is accompanied by both the sale (transfer of title) of a movable object (the roof shingles) and a service (the installation).[24] Except for potential future repairs, the roof is likely to fully function and serve its intended and ordinary purpose without the provision of additional ongoing services or software that tie directly to the roof's operability. In contrast, IoT devices are heavily software- and service-dependent objects and often rely on the provision of uninterrupted services from the device manufacturer to properly function. These continuous services and software updates go beyond the need for device repairs.

Consumer IoT devices can often be controlled and operated primarily through the mobile applications companies provide.[25] A Ring camera is only as useful as the mobile application that the company provides that allows the Ring owner to view the camera footage. IoT devices and the mobile applications connected to them often must receive updates from device manufacturers to continue to function properly and securely. Like the Ring camera, Nest consumers must use the company's mobile application or website to view real-time images and videos captured by their connected cameras, and the Nest Aware subscription service allows users to access older videos stored in the cloud via the mobile application or website.[26]

To deal with Article 2's historic lack of express guidance on hybrid transactions, the majority of courts use a predominant purpose test to determine whether Article 2 should apply to a transaction that involves both goods and non-goods.[27] Under the predominant purpose test, Article 2 and its accompanying warranty rules apply if the predominant purpose of the transaction is for the sale of goods as defined under Article 2.[28] Courts have used multiple factors when applying the predominant purpose test, including "the nature and reasonableness of the purchaser's contractual expectations of acquiring a property interest in

24. U.C.C. § 2-102 cmt. 4 (AM. L. INST. & UNIF. L. COMM'N 2022).

25. John Greenough, *The "Internet of Things" Report: How the Market Will Grow Across the Home, Enterprise, and Government Sectors*, BUS. INSIDER (Oct. 9, 2014), https://www.businessinsider.com/the-internet-of-things-is-rising-examining-the-internet-of-things-2014-9 [https://perma.cc/HP2W-N8GP].

26. *Nest Aware*, GOOGLE STORE, https://store.google.com/us/product/nest_aware?hl=en-US [https://perma.cc/2KBJ-XSLY]; *Watch Nest Camera's Video History on a Computer*, GOOGLE SUPPORT, https://support.google.com/googlenest/answer/9225631?hl=en [https://perma.cc/NF43-FK7A].

27. RUSCH ET AL., *supra* note 16, at 25; U.C.C. § 2-102 cmt. 2 (AM. L. INST. & UNIF. L. COMM'N 2022).

28. RUSCH ET AL., *supra* note 16, at 25.

goods"[29] and the "factual circumstances surrounding the negotiation, formation, and contemplated performance of the contract . . . ."[30] Courts' use of different factors when applying the predominant purpose test makes it potentially difficult to consistently determine with certainty prior to a lawsuit if a transaction that involves goods and non-goods is subject to Article 2.

The contract language and the parties' reasons for entering into a contract can also factor into a court's analysis of the predominant purpose as well as the cost of the movable goods in comparison to the services.[31] For example, Peloton reportedly remotely disabled a free-run feature on its connected treadmill that allowed consumers to use the device without paying a monthly subscription fee.[32] The responses of some Peloton customers suggest that they purchased the IoT treadmill because of the subscription services (class membership), with one customer stating, "The whole purpose of the treadmill is the subscription. The classes. The leaderboard. Who spends $3k and up on a subscription model device to not use it for that?"[33] For these customers, their primary reason for entering a contract for an IoT device was to obtain connected services rather than simply traditional goods. One might also contend that, in an IoT transaction, the price of the movable device often significantly outweighs any monthly subscription fees for connected services at the time of contracting. However, these monthly subscription fees could easily equal or exceed the purchase price of the device over time, depending on how long the consumer retains the device. Another factor that courts may consider in applying the predominant purpose test is "the nature of the seller's business."[34] Is a company like Peloton primarily in the business of providing movable objects, connected services, or both? The answer is not entirely clear.

Lastly, while a court may consider several factors in applying the predominant purpose test, as one court has observed, "[n]one of th[ose] factors alone is dispositive."[35] Consider the Amazon Dash Smart Shelf, a connected scale with "smart inventory tracking" capabilities that appear to go beyond traditional timed inventory replenishment and

---

29. Colo. Carpet Installation, Inc. v. Palermo, 668 P.2d 1384, 1389 (Colo. 1983).

30. Glover Sch. & Off. Equip. Co. v. Dave Hall, Inc., 372 A.2d 221, 223 (Del. Super. Ct. 1977).

31. Audio Visual Artistry v. Tanzer, 403 S.W.3d 789, 798 (Tenn. Ct. App. 2012).

32. Mary Hanbury, *Peloton Disabled a Free Feature on its $4,000 Tread+, Forcing Owners to Pay a $39 Monthly Fee to Use the Machine. Some Are Threatening Legal Action*, BUS. INSIDER (June 22, 2021, 12:11 PM), https://www.businessinsider.com/peloton-treadmill-customers-threaten-class-action-lawsuit-over-treadmill-membership-2021-6?amp [https://perma.cc/JY7M-K6WS].

33. *Id.*

34. Tanzer, 403 S.W.3d at 798.

35. *Id.* (quoting Pass v. Shelby Aviation, No. W1999-0001, 2000 WL 388775, at *4 (Tenn. Ct. App. Apr. 13, 2000)).

delivery services.[36] The device can automatically reorder products that the device determines are "running low" after the products are placed on the scale.[37] The shelf can be controlled via the Amazon shopping mobile app and appears to connect to the company's Dash Replenishment or Smart Reorders Service ("DRS").[38] Various device manufacturers have designed their devices to be DRS-enabled.[39] A customer who purchases the Amazon Dash Smart Shelf appears to obtain access not only to the movable scale but also to Amazon's smart reordering service, which "takes advantage of Amazon's payments systems, customer service, fulfillment network" and the company's mobile shopping app.[40] Such a transaction appears to involve both the provision of goods and non-goods and it therefore raises the question of whether the transaction should be subject to Article 2.

When applying the predominant purpose test to a transaction involving the purchase of the Amazon Dash Smart Shelf, one might posit that the predominant purpose of the transaction is for the provision of goods, a "movable" shelf or scale, and view any non-goods aspect to the transaction as incidental even if it is necessary for the goods to function. Thus, "necessity does not determine the predominant nature of the transaction."[41] An individual could, in theory, elect to buy the smart shelf without enabling the smart reordering features of the device. However, perhaps a more convincing argument is that an individual

---

36. *Dash Smart Shelf*, AMAZON, https://www.amazon.com/Dash-Smart-Shelf/dp/B07RV6X8LZ [https://perma.cc/ZM2M-SDRT]; *see also* Tom Ryan, *Will Amazon's Dash Smart Shelf Drive Auto-Replenishment from SMBs and Consumers?*, RETAILWIRE (Nov. 12, 2020), https://retailwire.com/discussion/will-amazons-dash-smart-shelf-drive-auto-replenishment-from-smbs-and-consumers [https://perma.cc/MRW7-YVA8].

37. Lauren Goode, *Review: Amazon Dash Smart Shelf*, WIRED (Mar. 8, 2021, 7:00 AM), https://www.wired.com/review/amazon-dash-smart-shelf [https://perma.cc/5EVV-JJES]; *Products You Can Reorder with Dash Smart Shelf*, AMAZON, https://www.amazon.com/b?ie=UTF8&node=21403320011 [https://perma.cc/W2Y7-5VRP].

38. *See Dash Smart Shelf*, *supra* note 36; Goode, *supra* note 37; *see also Amazon Dash Terms, Warranties, and Notices*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201741620 [https://perma.cc/T4Z4-94E3]; *Smart Reorders Promotional Terms & Conditions*, AMAZON, https://www.amazon.com/b?ie=UTF8&node=21417024011 [https://perma.cc/PV4B-EPYR].

39. *Jabil Joins New Amazon Dash Replenishment Service Providers Program*, JABIL (May 30, 2018), https://www.jabil.com/news/jabil-joins-new-amazon-dash-replenishment-service-providers-program.html [https://perma.cc/8M69-NNFG].

40. *Amazon Dash Replenishment FAQs*, AMAZON, https://developer.amazon.com/en-US/alexa/dash-services/faq [https://perma.cc/664X-LFZ4]; Liv Bez, *The Pros and Cons of the Amazon Dash Smart Shelf*, ROBOTICS & AUTOMATION (Aug. 20, 2021), https://roboticsandautomationnews.com/2021/08/20/the-pros-and-cons-of-the-amazon-dash-smart-shelf/45674 [https://perma.cc/C8ZA-X4VE]; Ishara Fernando, *Amazon Dash Smart Shelf – Smart Online Shopping*, NEWSBREAK (Nov. 11, 2016), https://original.newsbreak.com/@ishara-fernando-1590158/2435471683925-amazon-dash-smart-shelf-smart-online-shopping [https://perma.cc/LFM2-R9ME]; Goode, *supra* note 37; *Smart Reorders for Your Devices*, AMAZON, https://www.amazon.com/b?node=21076926011 [https://perma.cc/89WR-XSK2].

41. Bruel & Kjaer v. Vill. of Bensenville, 969 N.E.2d 445, 458 (Ill. App. Ct. 2012).

who chooses to purchase the Amazon Dash Smart Shelf instead of a non-IoT shelf or scale likely does so primarily to obtain access to the connected systems and software that enable automatic reordering and product consumption monitoring. Indeed, even if the reordering features associated with the shelf are not enabled, the device owner will likely still use the company's mobile app to make purchases, control device features, and receive notifications when products are running low. Thus, one could view the predominant purpose of the transaction as one for non-goods, thereby removing the transaction from Article 2's scope.

While most courts have adopted a predominant purpose standard to deal with hybrid transactions, some courts have used a bifurcation standard. Under a bifurcation approach, courts "distinguished the provisions in Article 2 that deal with the goods from those that deal with the transaction as a whole, and applied only the former in a hybrid transaction."[42]

The 2022 UCC Amendments to Article 2 attempt to provide express guidance on how to resolve hybrid transactions.[43] A "hybrid transaction," under the 2022 UCC Amendments, is a "single transaction involving a sale of goods and: (a) the provision of services; (b) a lease of other goods; or (c) a sale, lease, or license of property other than goods."[44] While this definition does not reference the term software, its reference to a license of property could potentially cover licenses of software associated with IoT devices. The 2022 UCC Amendments appear to adopt a combination of the predominant purpose approach and the bifurcation approach.[45]

Under the 2022 UCC Amendments, if the sale-of-goods portion of the transaction does not predominate over the non-goods aspect of the transaction, only the portions of Article 2 that "relate primarily to the sale-of-goods aspects of the transaction apply, and the provisions that relate primarily to the transaction as a whole do not apply."[46] If the goods aspect of the transaction predominates in the hybrid transaction, then Article 2 "applies to the transaction but does not preclude application in appropriate circumstances of other law to aspects of the

---

42. U.C.C. § 2-102 cmt. 2 (AM. L. INST. & UNIF. L. COMM'N 2022).

43. The ALI and ULC also previously attempted to address hybrid transactions involving software via the failed Article 2B project. 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); *see also* 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).

44. U.C.C. § 2-106(5) (AM. L. INST. & UNIF. L. COMM'N 2022).

45. *See* Foster v. Colo. Radio Corp., 381 F.2d 222 (10th Cir. 1967); TK Power, Inc. v. Textron, Inc., 433 F. Supp. 2d 1058 (N.D. Cal. 2006); Stephenson v. Frazier, 399 N.E.2d 794 (Ind. Ct. App. 1980).

46. *See* U.C.C. § 2-102.

transaction which do not relate to the sale of goods."[47] In seeking to codify aspects of both the predominant purpose and the bifurcation approach, the 2022 UCC Amendments appear to adopt a "two-tiered test."[48] To the extent that the goods portion of the transaction predominates in a hybrid transaction, Article 2 presumably applies to the entire transaction.[49] However, if the non-goods aspect of the transaction predominates, then the provisions of Article 2 associated with the sale of goods can apply only to the portion of the transaction involving the sale of goods.[50] Presumably, the common law of contracts and potentially other sources of law would apply to the remainder of the transaction.[51]

The two-tiered approach has several benefits. First, it ensures that, in a sale-of-goods transaction, a buyer can receive the benefit of the implied warranty of merchantability for the goods purchased, even if a court concludes that the predominant purpose of the transaction is not for the provision of those goods. Thus, in an IoT transaction involving a physical device and the simultaneous provision of services and software, Article 2 can apply to the "movable" or tangible components of the transaction. Under the traditional predominant purpose test, the question of whether an implied warranty of merchantability is applicable to the transaction is often lumped into the discussion of Article 2's application to the transaction. Second, the two-tiered approach does not appear to clearly depend on the essence, nature, or type of claim asserted by the plaintiff, thereby avoiding at least one pitfall associated with the gravamen of the claim standard under Article 2. The Article 2 gravamen of the claim standard employs an alternative approach to hybrid transactions that requires parties to wait until a claim is asserted or the source of the harm is clear before they can determine whether Article 2 and its accompanying warranties apply to a transaction.[52]

Despite potential benefits, the approach taken in the 2022 UCC Amendments raises several potential concerns. The 2022 UCC Amendments do not resolve the ambiguities associated with applying the predominant purpose test discussed earlier. The comments section incorporates several of the factors that courts have historically used to apply the predominant purpose test.[53] If a court determines that a transaction is predominantly for the provision of non-goods, then Article 2

47. *Id.*

48. *Id.* § 2-102 cmt. 2.

49. UNIF. L. COMM'N., A SUMMARY OF THE 2022 AMENDMENTS TO THE UNIFORM COMMERCIAL CODE 9 (2022), https://www.ndlegis.gov/files/committees/67-2021/23_9335_01000appendixb.pdf [https://perma.cc/KPQ8-UQFZ].

50. *Id.*

51. *See id.*

52. *See* Anthony Pools v. Sheehan, 455 A.2d 434, 440–41 (Md. 1983); J.O. Hooker & Sons, Inc. v. Roberts Cabinet Co., 683 So. 2d 396, 400 (Miss. 1996); WILLIAM D. HAWKLAND, UNIFORM COMMERCIAL CODE SERIES § 2-102 (2008); RUSCH ET AL., *supra* note 16, at 26.

53. U.C.C. § 2-102 cmt. 3 (AM. L. INST. & UNIF. L. COMM'N 2022).

likely applies only to some portions of the transaction rather than the entire transaction.[54]

The comments to the 2022 UCC Amendments indicate that the parties may agree in advance "that Article 2 will not govern the non-goods aspects of a hybrid transaction, even though the sale-of-goods aspects predominate. But, when sale-of-goods aspects predominate, the parties cannot agree that Article 2 does not govern matters that relate to the transaction as a whole, such as contract formation and enforceability."[55] The comments section goes on to provide as an example that in a transaction to "design, build and sell customized robotics . . . [t]he parties may, in their agreement, provide that Article 2 does not govern the services aspects of the transaction."[56]

These comments suggest that even if a court determines that the predominant purpose of the transaction is for the sale of goods, it is possible that the parties may agree in advance to limit Article 2's application to certain portions of the transaction. It appears that such a limitation may be possible even where the non-goods aspect of the transaction is integral to the operations of the goods that are sold, unless the limitation is viewed as an impermissible attempt to limit Article 2's application to "matters that relate to the transaction as a whole."[57] This approach presumes that the non-goods and goods aspects of a transaction can be consistently and easily separated from ongoing device functionality in the same way that services to build and design goods can be separated from the final goods upon completion of contracted-for services. It also fails to recognize the central role that the non-goods aspect of a transaction plays in IoT device functionality and safety. As a result, the non-goods aspect of the transaction, even if essential to device functionality, may not consistently fall under Article 2's implied warranties — a technicality that may have important privacy and cybersecurity implications. Thus, if a cybersecurity vulnerability occurs that is not clearly connected to the physical device but is associated with the company's online services, software, and systems, the implied warranties may not apply to that portion of the transaction. On the other hand, Article 2's implied warranties would presumably apply to a cybersecurity vulnerability that led to exfiltration of data directly from the physical movable device or if a hacker exploits a device vulnerability that allows the hacker to control an individual's device. We will return to the issue of cybersecurity below.

---

54. *Id.* § 2-102 cmt. 5.

55. *Id.* § 2-102 cmt. 6. ("The rules of subsections (1) and (2) are essentially gap fillers that apply when the parties' agreement is silent on what legal rules govern the different aspects of their transaction."). This approach is not surprising as the UCC has historically given parties the ability to "vary the effect of many of [its] provisions" by agreement. RUSCH ET AL., *supra* note 16, at 10–11; U.C.C. § 1-302 (AM. L. INST. & UNIF. L. COMM'N 2022).

56. U.C.C. § 2-102 cmt. 6 (AM. L. INST. & UNIF. L. COMM'N 2022).

57. *Id.*

Another possible shortcoming of the 2022 UCC Amendments is that the definition of hybrid transactions is limited to a "single transaction."[58] In the IoT context, consumers are likely to be subject to multiple agreements to ensure that their devices continue to function. Depending on the nature of the transaction, in addition to agreeing to a contract for the sale of the physical device, the consumer may also be subject to the company's terms of service with respect to any subscription services or any mobile applications used to control the device. For example, historically a consumer who purchased an IoT Nest product directly from the online Nest store would be subject to Nest's terms and conditions of sale[59] for the movable device; terms of service for the accompanying mobile application, website, and subscription services;[60] a limited warranty for the device;[61] an end-user license agreement[62] for embedded software; and a privacy policy.[63]

The comments to the 2022 UCC Amendments indicate that "if contracting parties enter into separate agreements at the same time, each agreement creating a separate transaction, each transaction must be evaluated separately to determine if it is a hybrid transaction."[64] The comments suggest that, in some cases, a separate agreement for a transaction for services may not create a hybrid transaction.[65] Thus, it is possible that the subscription services and mobile app services connected to device functionality could constitute separate agreements rather than a hybrid transaction potentially subject to Article 2. This gap leaves significant room for companies to structure the transaction to avoid application of Article 2 and its implied warranties.

Consumers may also fall subject to multiple terms of service when a corporate reorganization occurs. For instance, after Nest merged into Google's hardware division and lost its status as a "standalone Alphabet company,"[66] to use newer Nest devices, such as the Nest Doorbell,

---

58. *See id.* § 2-106(5).

59. *Sales Terms, Terms & Conditions of Sale*, NEST, https://nest.com/legal/sales-terms [https://perma.cc/L4B6-PLVM].

60. *Terms of Service*, NEST, https://nest.com/legal/terms-of-service [https://perma.cc/2UHE-DJCK] (last updated Mar. 5, 2020).

61. *Limited Warranty*, NEST, https://nest.com/legal/warranty [https://perma.cc/E86L-FERY].

62. *End User License Agreement*, NEST, https://nest.com/legal/eula [https://perma.cc/V4ST-7HEB].

63. *Privacy Policy for Nest Web Sites*, NEST, https://nest.com/legal/privacy-policy-for-nest-web-sites [https://perma.cc/FW49-MG2T]; *see also Privacy Policy for Nest Products and Services*, NEST, https://nest.com/legal/privacy-statement-for-nest-products-and-services [https://perma.cc/B5W4-TKQN].

64. U.C.C. § 2-106 cmt. 5 (AM. L. INST. & UNIF. L. COMM'N 2022).

65. *Id.*

66. Ron Amadeo, *Nest Is Done as a Standalone Alphabet Company, Merges with Google*, ARS TECHNICA (Feb. 7, 2018, 3:05 PM), https://arstechnica.com/gadgets/2018/02/nest-is-done-as-a-standalone-alphabet-company-merges-with-google/amp [https://perma.cc/F97Q-7FA6].

users had to consent to both Google's terms of service and Nest's additional terms of service.[67]

One potential alternative solution to the hybrid transactions problem is to adopt a functional test to determine when Article 2 should apply to a hybrid transaction. Under this approach, Article 2 would apply to physical IoT devices as well as the services and software connected to device functionality. If an IoT device cannot fully operate without the associated services and software, the transaction should be subject to Article 2. In making this determination, a court could evaluate how manufacturers and retailers advertise the IoT device to consumers in addition to how essential the software and services are to the operations of the device.

One potential critique of this approach is that implied warranties should apply to goods rather than services or software. However, implied warranties are not entirely foreign to service contracts. In *Welwood v. Cypress Creek Estates, Inc.*,[68] the court observed that there is an implied warranty for services "when the services relate to the repair or modification of existing tangible goods or property."[69] Thus, implied warranties can arguably extend to service contracts as a matter of public policy in compelling circumstances to ensure that consumers have an adequate remedy.[70] With respect to software, the Uniform Computer Information Transactions Act — a model law governing software licensing — extends the implied warranty of merchantability to certain software transactions.[71] The ALI's Software Principles also contain a non-disclaimable "implied warranty of no hidden material defects."[72] In other words, there are various sources of law that contemplate enforcing implied warranties in service and software transactions.

---

67. *Nest Additional Terms of Service*, GOOGLE SUPPORT, https://support.google.com/product-documentation/answer/9327735 [https://perma.cc/5BYU-CR4G]; *see also Create a New Account to Use the Nest App*, GOOGLE SUPPORT, https://support.google.com/googlenest/answer/10503498?hl=en [https://perma.cc/EL3C-K4BR].

68. 205 S.W.3d 722 (Tex. App. 2006).

69. *Id.* at 730; Rocky Mountain Helicopters v. Lubbock Cnty. Hosp. Dist., 987 S.W.2d 50, 52–53 (Tex. 1998) (citing Melody Home Mfg. Co. v. Barnes, 741 S.W.2d 349, 354 (Tex. 1987); *see also* Uniform Computer Information Transactions Act § 403 cmt. 1 (NAT'L CONF. OF COMM'RS ON UNIF. STATE L. 2002).

70. *Welwood*, 205 S.W.2d at 730.

71. UNIF. COMPUT. INFO. TRANSACTIONS ACT § 403 (NAT'L CONF. OF COMM'RS ON UNIF. STATE L. 2002).

72. AM. L. INST., PRINCIPLES OF THE LAW OF SOFTWARE CONTRACTS § 3.05(b) (2010); *see also* Robert A. Hillman & Maureen O'Rourke, *Principles of the Law of Software Contracts*, 84 TUL. L. REV. 1519, 1519–20, 1537 (2010).

III. EXPLORING THE CONTOURS OF THE MERCHANTABILITY WARRANTY

To succeed on a breach of the implied warranty of merchantability claim, a buyer must show, among other things, that the goods sold were not merchantable.[73] One of the core purposes of the merchantability warranty is the promotion of fair dealing by merchants with respect to the goods they sell.[74] Another important goal of the merchantability warranty is to ensure the protection of the reasonable expectations of buyers who purchase goods from merchants.[75] As the FTC has noted, when consumers "buy IoT devices, they generally expect that the things they buy will work and keep working, and that security controls have been established as a default."[76] The FTC has also noted that "when a product is sold, there is an implied representation that the product is fit for the purpose for which it is sold. When it is not, deception occurs" in violation of the FTCA.[77] The FTC has indicated that this implied

---

73. JAMES J. WHITE & ROBERT S. SUMMERS, UNIFORM COMMERCIAL CODE 480–81 (6th ed. 2010) ("Under 2-314, a plaintiff must prove that (1) a merchant sold goods, (2) which were not 'merchantable' at the time of sale, (3) there was damage to the plaintiff or its property (4) caused proximately and in fact by the defective nature of the goods, and (5) notice to seller of injury."). On the issue of causation, although "the plaintiff normally must show more than that the goods injured the plaintiff in a certain way . . . it is not always necessary that the plaintiff offer expert testimony or explicit proof to disclose the precise chain of causation . . . [and] when the connection between the product and the injury is reasonably obvious even to a layman, expert proof and explicit analysis of the chain of causation should not be necessary." *Id.* at 494–95. Privity concerns may also arise in implied warranty claims when a buyer seeks to bring a claim against a remote seller. *Id.* at 481 (discussing the merchantability warranty and noting that "the non-privity buyer also cannot recover for economic loss from a remote manufacturer"); DAVID G. OWEN, PRODUCTS LIABILITY LAW 187 (West Academic 3d ed. 2015) (same). However, some courts have recognized exceptions to the privity requirement that may be useful for plaintiffs attempting to bring implied warranty claims. *E.g.*, *In re* VTech Data Breach Litig., Nos. 15-10889, 15-10891, 15-11620, 15-11885, 2018 U.S. Dist. LEXIS 65060, at *18 (N.D. Ill. Apr. 18, 2018). Additionally, the IoT weakens justifications for the maintenance of privity requirements in breach of implied warranty claims involving IoT devices, particularly since device owners are likely to rely heavily on continued services and software updates from device manufacturers for ongoing device functionality. *See* Bosson, *supra* note 3.

74. OWEN, *supra* note 73, at 167.

75. *Id.* (discussing the merchantability warranty and noting that "[i]ts foundation lies in public policy, in order to promote fair dealing by sellers of chattels, and to protect fair expectations of buyers of goods"); *In re* Carrier IQ, Inc., Consumer Priv. Litig., 78 F. Supp. 3d 1051, 1107 (N.D. Cal. 2015); s*ee also* DOUGLAS J. WHALEY & STEPHEN M. MCJOHN, PROBLEMS AND MATERIALS ON COMMERCIAL LAW 138 (Aspen Publishing 11th ed. 2016); RUSCH ET AL., *supra* note 16, at 189.

76. *Careful Connections: Keeping the Internet of Things Secure*, FTC (Sept. 2020), https://www.ftc.gov/business-guidance/resources/careful-connections-keeping-internet-things-secure [https://perma.cc/W8VG-2N44] [hereinafter *Careful Connections*].

77. Letter from James C. Miller III, Chairman, FTC, to John D. Dingell, Chairman, House Comm. on Energy & Com. (Oct. 14, 1983), http://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/Z7XN-A3HT].

representation shares similarities with the UCC's merchantability warranty.[78]

The average buyer of an IoT device may expect that IoT companies have adopted robust methods to ensure that their devices, related services and systems, and the data the devices collect are reasonably secure. Indeed, data security is an integral part of IoT device functionality and IoT companies' online services and products.[79] Oftentimes, IoT devices, by design, function in part by collecting data about the user and the device's surroundings.[80] Thus, a core purpose of the smart features of IoT devices is to collect and process data about individuals. It is reasonable to infer that the average IoT device user expects that the company collecting and processing these data will keep the data secure and consider consumer privacy when designing such devices. Indeed, in denying a motion to dismiss a claim for breach of the implied warranty of merchantability, the United States District Court for the Northern District of California in *In re Carrier IQ, Inc.*[81] reasoned that "consumers have a reasonable expectation that mobile devices, in general, will allow them to communicate with others without having a third party surreptitiously intercept and transmit those communications to third parties."[82] IoT device owners likely have a similar expectation of privacy, particularly since many IoT devices are controlled through mobile apps that consumers access on their smartphones.

Article 2 provides express non-exhaustive guidance on determining whether goods are merchantable. Although merchantable goods need not be absolutely perfect, they must be "fit for the ordinary purpose for which such goods are used"[83] and "safe for their ordinary uses."[84] The implementation of robust cybersecurity measures is a key component of the safety of IoT devices. An IoT device with related systems and services that collect and store data vulnerable to cybersecurity intrusion could, in certain instances, fail to qualify as fit for its ordinary purpose.[85] If a cybersecurity vulnerability in an IoT device or

78. *In re* Int'l Harvester Co., 104 F.T.C. 949, 1058 n.35 (1984).

79. U.S. DEP'T OF JUST. CYBERSECURITY UNIT, SECURING YOUR "INTERNET OF THINGS" DEVICES 1–3 (2017), https://www.justice.gov/criminal-ccips/page/file/984001/download [https://perma.cc/HX7U-NXPD].

80. *See* Patrick McFadin, *Internet of Things: Where Does the Data Go?*, WIRED (Mar. 2015), https://www.wired.com/insights/2015/03/internet-things-data-go/#comment-1896738214 [https://perma.cc/2AKJ-S7PY]; *e.g.*, Lily Hay Newman, *Why Ring Doorbells Perfectly Exemplify the IoT Security Crisis*, WIRED (Dec. 12, 2019), https://www.wired.com/story/ring-hacks-exemplify-iot-security-crisis [https://perma.cc/26L4-93LJ].

81. *In re* Carrier IQ, Inc. Consumer Priv. Litig., 78 F. Supp. 3d 1051 (N.D. Cal. 2015).

82. *Id.*

83. WHITE ET AL., *supra* note 73, at 491; U.C.C.§ 2-314(2)(c) (AM. L. INST. & UNIF. L. COMM'N 1995).

84. OWEN, s*upra* note 73, at 171–72 (citing ROBERT J. NORDSTROM, LAW OF SALES § 76, at 236 (West Publishing 3d ed. 1970)).

85. *See* Shooshanian v. Wagner, 672 P.2d 455 (Alaska 1983); Bernard v. Dresser Indus., Inc., 691 S.W.2d 734 (Tex. App. 1985); *see also* WHITE ET AL., *supra* note 73, at 490.

connected service is exploited in a manner that causes harm, the device could be viewed as defective, regardless of whether the device continues to have a base level of functionality after the cybersecurity incident.[86] Courts have noted that although there must be an important defect "that renders the product unfit for its ordinary purpose. . . . [a]t the same time, this does not mean the alleged defect must preclude any use of the product at all."[87]

In addition to legal frameworks that may mandate or encourage companies to adopt privacy and security by design principles, the implied warranty of merchantability could serve as an alternative avenue for the promotion of privacy and security by default and by design principles. Comment 6 to Section 2-314 expressly notes that the drafters intended "to leave open other possible attributes of merchantability."[88] In the digital age, privacy and cybersecurity are key aspects of contemporary goods and as such should be viewed as modern attributes of the merchantability warranty. Exposure to liability via direct lawsuits from consumers can serve as a powerful incentive to encourage companies to design devices and maintain services and networks with security in mind and adopt appropriate data collection practices.

Factors to consider[89] in determining whether a device is fit for its ordinary purpose include whether the company (1) has built security and privacy into the device and related services and systems at multiple stages, including evaluating concerns associated with using multiple TPCs;[90] (2) uses distinctive rather than repetitive default passwords that the end user is required to change during device set up; (3) implements robust multifactor authentication and encryption methods, such as configuring controls to ensure the security of master encryption keys;[91] (4) has taken steps to avoid and timely remedy known

86. *In re* Carrier IQ, Inc., 78 F. Supp. 2d at 1109.

87. Stearns v. Select Comfort Retail Corp., No. 08-2746, 2009 U.S. Dist. LEXIS 48367, at *25 (N.D. Cal. June 5, 2009); *see also id.* at 1110–11; Long v. Graco Children's Prods., No. 13-01257, 2013 U.S. Dist. LEXIS 121227 (N.D. Cal. Aug. 26, 2013); Roberts v. Electrolux Home Prods., No. 12-1644, 2013 U.S. Dist. LEXIS 185488 (C.D. Cal. Mar. 4, 2013); Fleisher v. Fiber Composites, LLC, No. 12-1326, 2012 U.S. Dist. LEXIS 157343 (E.D. Pa. Nov. 2, 2012); Isip v. Mercedes-Benz USA, LLC, 155 Cal. App. 4th 19 (Cal. Ct. App. 2007). *But see* Williamson v. Apple, Inc., No. 11-00377, 2012 U.S. Dist. LEXIS 125368 (N.D. Cal. Sept. 4, 2012); *In re* iPhone 4S Consumer Litig., No. 12-1127, 2013 U.S. Dist. LEXIS 103058 (N.D. Cal. July 23, 2012).

88. U.C.C. § 2-314 cmt. 6 (AM. L. INST. & UNIF. L. COMM'N 2021).

89. *See, e.g.*, *Careful Connections*, *supra* note 76.

90. Natali Tshuva, *The Hidden Risk in All IoT Devices: Third-Party Components*, STERNUM (June 25, 2019), https://sternumiot.com/iot-blog/the-hidden-risk-in-all-iot-devices-third-party-components [https://perma.cc/3DHW-PS5X].

91. Despite the use of robust encryption methods, the risk that data may be de-encrypted may still remain. Consideration could be given to which contractual party (consumers or the firms that collect and store consumer data) is best suited to bear the risk of decryption. *See, e.g.*, Stephen Shankland, *Quantum Computers Could Crack Todays' Encrypted Messages.*

cybersecurity vulnerabilities, such as deploying "automatic security patches"; (5) on an ongoing basis, conducts cybersecurity testing of systems and services connected to IoT device functionality through the expected life cycle of the device; (6) complies with applicable state and federal regulation, if any;[92] (7) implements, when applicable, notable cybersecurity guidance for IoT devices, such as those issued by the National Institute for Standards and Technology ("NIST"), if any; (8) implements frequent privacy and data security training for employees; and (9) adopts procedures to ensure that service providers and third parties with access to IoT device users' data maintain adequate privacy and security measures.[93]

One could argue that complicated IoT software supply chain issues, including those associated with TPCs and device integration, may hinder firms' ability to maintain and ensure a basic level of cybersecurity in IoT devices.[94] Following this line of argument, use of these factors and potential resulting merchantability liability may decrease efficiency by lengthening product development time frames. However, companies should be selective and thoughtful in evaluating software supply chain issues and related privacy and cybersecurity concerns. As one legal scholar has observed, "the implied warranty of merchantability is the most basic warranty that every manufactured product must meet. It is simply common sense that no manufacturer should make and sell a product that is not fit for its ordinary purpose."[95] In the IoT age, fit for the ordinary purpose requires some basic level of privacy and

---

That's a Problem, CNET (May 24, 2021), https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem [https://perma.cc/78QQ-HAHV] (discussing quantum computers that could "crack much of today's encryption"); *see also* Eric Blattberg, *Target Backpedals: Hackers Stole PIN Data in Breach*, VENTUREBEAT (Dec. 27, 2013), https://venturebeat.com/security/target-hackers-stole-pin-data-in-breach [https://perma.cc/6PNB-T4YU] (noting that data thieves could crack encrypted data even if encryption keys were not disclosed, which could result in misuse of consumer data).

92. The relevance of this factor could depend on whether the applicable legislation expressly precludes private causes of action based on statutory violations.

93. *See Careful Connections*, *supra* note 76; FTC STAFF REPORT, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/6L6N-FGSK]; *see also* Uniform Computer Information Transactions Act § 403, cmt. 3 (NAT'L CONF. OF COMM'RS ON UNIF. STATE L. 2002); NAT'L INST. FOR STANDARDS & TECH., FOUNDATIONAL CYBERSECURITY ACTIVITIES FOR IOT DEVICE MANUFACTURERS (2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf [https://perma.cc/8CLE-HPPH].

94. *See* Toby Mills, *Supply Chain Disruption: Why IoT Is Failing to Join the Dots*, VENTUREBEAT (Oct. 20, 2022), https://venturebeat.com/data-infrastructure/supply-chain-disruption-why-iot-is-failing-to-join-the-dots [https://perma.cc/L9LR-GT3K]; Stacia Lee, *Internet of Things Device Security and Supply Chain Management*, U. WASH. (Mar. 12, 2017), https://jsis.washington.edu/news/verifying-internet-things-device-security-good-housekeeping-supply-chain-management [https://perma.cc/UY4M-Z7X2].

95. Ralph C. Anzivino, *The Implied Warranty of Merchantability and the Remote Manufacturer*, 101 MARQ. L. REV. 505, 526 (2017).

cybersecurity to be built into a device and related services, software, and systems.

Article 2 also provides that for goods to be merchantable they must "conform to the promise or affirmations of fact made on the container or label if any."[96] Promises or representations made by a company about the security and privacy features of an IoT device could be relevant in assessing merchantability claims. The comments to Section 2-314 note that the obligation that goods must "conform to the promise or affirmations of fact made on the container or label" to be merchantable flows "from the general obligation of good faith which requires that a buyer should not be placed in the position of . . . using goods delivered under false representations appearing on the package or container."[97]

The affirmations of fact and promises standard also shares some similarities with the FTC's approach to its FTCA authority. Although a privacy policy may not qualify as a contract, the FTC has pursued companies for failure to adhere to their privacy and data security promises.[98] Similarly, the implied warranty of merchantability could in some instances be interpreted to provide IoT device owners with a cause of action in cases in which the company fails to meet its promises and affirmations of fact regarding data security and privacy made in connection with the sale of an IoT device and related services.

The term "label" as used in Section 2-314 could be interpreted broadly to cover not just the physical box or carton accompanying the IoT devices, but also the online promises and affirmations of fact made by companies in connection with the sale of such devices and the provision of related online services.[99] This interpretation could be

96. U.C.C. § 2-314(2)(f) (AM. L. INST. & UNIF. L. COMM'N 2001).

97. *Id.* § 2-314 cmt. 10; RUSCH ET AL., *supra* note 16, at 129.

98. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 595–97, 628–29 (2014). *But see* Oren Bar-Gill, Omri Ben-Shahar & Florencia Marotta-Wurgler, *Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts*, 84 U. CHI. L. REV. 7, 28 (2017) (finding that "privacy policies are typically recognized as contracts"); Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REG. 45, 50, 67 (2019).

99. Article 2 could also be amended to broadly define "label" or "container" to achieve this goal. One potential critique of this approach is that to the extent that the basis of a claim for breach of the implied warranty of merchantability depends in part on the failure of goods to conform to promises that involve or that are made by a third party, one might argue that such a claim may run afoul of Section 230 of the Communications Decency Act ("CDA"), which may limit a company's liability for speech published by third parties. *See* 47 U.S.C. § 230(c)(1) (2019); *see also* Erie Ins. Co. v. Amazon.com Inc., No. 16-02679, 2018 WL 3046243, at *3 (D. Md. Jan. 22, 2018). However, as Nancy Kim observes most "[c]laims based upon contract or breach of warranty do not implicate [S]ection 230 because they are not based upon content posted by others. Instead, the claims are based upon the company's own statements about its products and services." Kim, *supra* note 20, at 383. Additionally, at least one court has found that the CDA does not prohibit a breach of implied warranty claim

particularly useful in instances in which IoT devices are accompanied by layered labelling. Such labelling typically involves the inclusion of both a physical label describing the device's features and the accompanying cybersecurity or privacy standards, as well as a URL or Quick Response Code ("QR Code") on the label or container that the consumer can use to access additional information about the privacy and cybersecurity of the IoT device and associated services. NIST has recommended a similar approach to IoT device manufacturers.[100] To the extent that companies widely adopt this approach, promises and statements made via such disclosures could factor into the determination of whether a company has breached the implied warranty of merchantability.

Promises on a website could also be viewed as relevant, particularly when the consumer purchases the product online and considers the online descriptions and affirmations of fact on the company's website about IoT devices and service. Comment 2 to Section 2-714 of the UCC indicates that a buyer may sue for breach of warranty as well as "collateral promises of timely performance or the like."[101] This approach to the implied warranty of merchantability is also in keeping with the FTC's enforcement of implied and explicit privacy promises. The FTC has evaluated promises made by firms contained elsewhere on a company's website in addition to promises made in the privacy policy.[102]

In a claim for breach of the implied warranty of merchantability, the plaintiff must also successfully allege damages.[103] Article 2

---

against an online retailer "to the extent that a plaintiff may prove that an interactive computer service played a *direct* role in [the alleged] . . . conduct — through its involvement in the sale or distribution of the defective product." McDonald v. LG Elecs. USA, Inc., 219 F. Supp. 3d 533, 537–40 (2016) (finding that "plaintiff's negligence and breach of implied warranty claims (Counts VI and VII)" are not barred under the [CDA] because the plaintiffs "allege that Amazon is directly liable for its own . . . conduct").

100. NAT'L INST. FOR STANDARDS & TECH., RECOMMENDED CRITERIA FOR CYBERSECURITY LABELING FOR CONSUMER INTERNET OF THINGS (IOT) PRODUCTS 18–19 (2022), https://csrc.nist.gov/publications/detail/white-paper/2022/02/04/criteria-for-cybersecurity-labeling-for-consumer-iot-products/final [https://perma.cc/9KVR-4VNT].

101. WHITE ET AL., *supra* note 73, at 525 ("An aggrieved buyer will often seek general or direct damages for seller's breach of warranty under 2–714(1) and (2). The buyer may also sue for seller's breach of collateral promises of timely performance or the like."); U.C.C. § 2-714 cmt. 2 (AM. L. INST. & UNIF. L. COMM'N 2021).

102. Solove et al., *supra* note 98, at 629–30. A seller's online privacy and data security promises and affirmations of fact could also matter for purposes of alleging claims of breach of an express warranty. Unlike a claim for breach of an express warranty, in which reliance on the seller's representations may need to be shown to prove that the statement is part of the basis of the bargain, a buyer alleging breach of the implied warranty of merchantability does not have to show reliance on the representations or affirmations made by a seller to be successful. WHITE ET AL., *supra* note 73, at 482. *But see* U.C.C. § 2-313 cmt. 3 (suggesting that reliance is not always necessary to create an express warranty).

103. WHITE ET AL., *supra* note 73, at 480, 525. Mere data disclosure without more may not be consistently viewed as a cognizable harm. *See* Rudgayzer v. Yahoo! Inc., No. 12-01399, 2012 U.S. Dist. LEXIS 161302, at *18 (N.D. Cal. Nov. 9, 2021); Daniel J. Solove & Danielle

provides guidance on assessing damages in breach of warranty claims.[104] Article 2's provisions can be interpreted to cover various types of harm that IoT device owners may incur when companies fail to live up to their privacy and data security promises. Cybersecurity vulnerabilities can result in more than mere inconvenience to buyers.[105] A hacker could exploit a single IoT device's vulnerabilities to access all other devices connected to the insecure device.[106] IoT device owners who fall victim to a cybersecurity failure may not have received the value of the quality of the goods promised by the merchant, may incur costs associated with replacing and repairing defective devices, and in some cases may have paid a premium for insecure IoT devices (overpayment) and lost the option to buy less expensive goods and

---

K. Citron, *Privacy Harms*, 101 B.U. L. REV. 793, 808 (2022). *But see In re* Facebook Priv. Litig. v. Facebook, Inc., 572 Fed. Appx. 494, 496 (2014); Allison Grande, *9th Circ. Eases Data-Sharing Risks for Facebook, Others*, LAW360 (May 16, 2014, 9:34 PM EST), https://www.law360.com/articles/538749/9th-circ-eases-data-sharing-risks-for-facebook-others [https://perma.cc/N3M4-7P7M]. The issue of harm or injury is also connected to standing requirements. Alissa del Riego, *Deconstructing Fallacies in Products Liability Law to Provide a Remedy for Economic Loss*, 58 AM. BUS. L.J. 387, 411–12 (2021). The Supreme Court's most recent standing case, *TransUnion LLC v. Ramirez*, has made it significantly more difficult for plaintiffs to survive standing challenges in federal courts. 141 S. Ct. 2190 (2021); Daniel J. Solove & Danielle K. Citron, *Standing and Privacy Harms: A Critique of TransUnion v. Ramirez*, 101 B.U. L. REV. ONLINE 62, 69–71 (2021) (suggesting that plaintiffs may be unable to survive Article III standing challenges if they allege solely a risk of harm flowing from a data breach without sufficiently alleging data misuse that results in injury); However, the Court in *TransUnion* noted that "with respect to the concrete-harm requirement in particular, . . . *Spokeo v. Robins* . . . does not require an exact duplicate in American history and tradition." *TransUnion LLC*, 141 S. Ct. at 2204. The TransUnion Court further indicated that plaintiffs who are victims of "traditional tangible harms, such as physical harms and monetary harms . . . [have suffered] a concrete injury in fact under Article III." *Id.* at 2204. At least one federal court applying the *TransUnion* case has concluded that plaintiffs who overpaid for a defective vehicle and who were alleging a breach of the implied warranty of merchantability, among other things, suffered an injury in fact for standing purposes. Siqueiros v. GM LLC, No. 16-07244, 2021 U.S. Dist. LEXIS 169326 (N.D. Cal. Sept. 7, 2021); *see also* Withrow v. FCA US LLC, No. 19-13214, 2021 U.S. Dist. LEXIS 114908, at *31 (E.D. Mich. June 21, 2021) (finding that plaintiff has standing to pursue a breach of implied warranty claim in federal court because the "alleged injury (the purchase of an unmerchantable Ram) is fairly traceable to the challenged conduct (Fiat-Chrysler's manufacture and sale of an unmerchantable Ram that was ultimately sold to Withrow in New Jersey)"); *In re VTech Data Breach Litig.*, 2017 U.S. Dist. LEXIS 103298, at *17–18 ("[E]conomic injury can result from being given a different, less valuable product than the one that was promised and paid for, and such an injury meets Article III's injury-in-fact requirement."). Lastly, even if federal standing requirements constrain the viability of privacy and cybersecurity claims in federal courts, state courts may be a more hospitable venue for privacy and data security claims as state courts are not restricted by the Article III standing prerequisites. Thomas B. Bennett, *The Paradox of Exclusive State-Court Jurisdiction Over Federal Claims*, 105 MINN. L. REV. 1211, 1212–13 (2021).

104. U.C.C. § 2-714(2)–(3).

105. *In re* Google Phone Litig., No. 10-01177, 2012 WL 3155571, at *5 (N.D. Cal. Aug. 2, 2012).

106. *Careful Connections*, *supra* note 76.

services.[107] IoT cybersecurity victims may incur financial costs and suffer economic loss associated with credit monitoring, and may become exposed to an increased risk of reputational and relationship harm, as well as identity theft, and fraud.[108] These individuals may also experience depression, fear, and anxiety associated with concerns about the future emotional and financial impact of a data breach or insecure IoT device.[109] Service interruptions associated with core IoT device functions that might flow from cybersecurity vulnerabilities could result in other types of harm as well. For instance, hacking into an IoT thermostat could cause device and temperature malfunctions that

107. Complaint at 38–40, Gutierrez v. Samsung Elecs. Am. Inc., No. 22-05719, 2022 WL 15398352 (N.D. Cal. Oct. 27, 2022); WHITE ET AL., *supra* note 73, at 446 (defining economic loss).

108. *See In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 954–59 (S.D. Cal. 2014); *see also* Complaint, Seirafi et al. v. Samsung Electronics America Inc., No. 22-05176 (N.D. Cal. Feb. 2, 2023) (class action suit); Daniel Solove & Danielle K. Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737 (2018); Solove et al., *Privacy Harms*, *supra* note 103, at 843–44 (2022).

109. *See* Solove et al., *Privacy Harms*, *supra* note 103, at 808; *see also* Ido Kilovaty, *Psychological Data Breach Harms*, 23 N.C. J. L. & TECH. 1 (2021). With respect to the issue of anxiety and emotional harms, a potentially relevant issue may flow from some courts' reluctance to recognize harms beyond economic loss in claims for breach of contract. Article 2 indicates that in special circumstances a purchaser is permitted to recover for his loss "in any manner which is reasonable." U.C.C. § 2-714(1); WHITE ET AL., *supra* note 73, at 525–26 ("If the nonconformity was a breach of warranty, 2-714(2) — a subset of 2-714(1) — provides a measure that will adequately compensate the accepting buyer in many, but not all cases. When not, the buyer is told in Comment 2 that 2-714(2) is not an exclusive measure and the buyer may recover under the 'unless' clause of 2-714(2) or under 2-714(1) itself.") Further, as Daniel Solove and Danielle Citron have observed, although historically courts have been slow to acknowledge emotional harms in contract law, "they have shifted on this issue to move toward a greater allowance of recovery for emotional harm." Solove et al., *Privacy Harms*, *supra* note 103, at 843*; see also* WHITE ET AL., *supra* note 73, at 525–37 (contending that "2-715(2) codifies the more generous reading of *Hadley v. Baxendale*. Most of the courts have recognized that a seller is liable for all damages resulting from their breach if they arise from circumstances that the seller knew about or had reason to know about, even if the seller did not consciously assume the risk of such liability"); Mara Kent, *The Common-Law History of Non-Economic Damages in Breach of Contract Actions Versus Willful Breach of Contract Actions*, 11 TEX. WESLEYAN L. REV. 481, 486–93 (2005) (noting that one exception to the *Hadley* rule is "when the breach is willful or wanton in nature or if the breach causes bodily harm"). Additionally, on the topic of increased risk of damage or harm, courts' application of the manifest defect rule may pose a hurdle for warranty claims. *See* Briehl v. Gen. Motors Corp., 172 F.3d 623, 628 (8th Cir. 1999); Everett v. TK-Taito, L.L.C., 178 S.W.3d 844, 855 (Tex. App. 2005). However, at least one court has found that a risk of device failure or damage can be sufficient to sustain a breach of implied warranty claim. *See* Holtzman v. Gen. Motors Corp., No. 021368, 2002 WL 1923883 (Mass. Super. Ct. July 2, 2002). *But see* John F. Kuppens, Jay T. Thompson & James B. Glen, *The No-Injury Warranty Claims Quandary*, LAW360 (Dec. 13, 2021, 5:22 PM EST), https://www.law360.com/articles/293153/the-no-injury-warranty-claims-quandary [https://perma.cc/P9BX-AXY7] (critiquing the *Holtzman* case).

generate property damage, such as burst pipes in device owners' homes and health concerns for elderly or ill homeowners.[110]

Several courts have noted that "[a]n implied warranty of merchantability applies to the condition of the goods at the time of sale and is breached only if the defect in the goods existed when the goods left the seller's control."[111] To successfully allege a breach of the implied warranty of merchantability, a buyer may need to prove that the cybersecurity or privacy-related vulnerability existed at the time of sale.[112] This requirement could create a hurdle to the effective application of the implied warranty of merchantability in the IoT context. Cybersecurity vulnerabilities could arise over time rather than when the device left the company's control. Recall that, in the IoT setting, companies provide ongoing services and device support connected to device functionality. As such, certain firms that provide ongoing services will retain some control over such devices. Cybersecurity services may need to occur over time to remedy new vulnerabilities that arise after purchase. The implied warranty of merchantability can evolve to clearly recognize this development.

The current approach to warranty disclaimers could also arguably constitute a roadblock to consumers' effective use of the implied warranty of merchantability. Article 2 allows merchants who make the implied warranty of merchantability to disclaim the warranty upon meeting certain requirements.[113] One response to critiques regarding warranty disclaimers is that both existing federal law and state law can limit the effectiveness of warranty disclaimers. For instance, to address the warranty disclaimer and other remedies issues, "at least sixteen states and the District of Columbia" have adopted laws "prohibiting or restricting disclaimers and/or limitations of remedy" in consumer goods transactions.[114] More states could consider imposing restrictions on the disclaimer of implied warranties.

---

110. Nick Bilton, *Nest Thermostat Glitch Leaves Users in the Cold*, N.Y. TIMES (Jan. 13, 2016), https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html [https://perma.cc/P7HL-7J2N]; *see also* U.C.C. § 2-715(2) (defining consequential damages to include "injury to person or property proximately resulting from any breach of warranty").

111. Oggi Trattoria & Caffe, Ltd. v. Isuzu Motors Am., Inc., 865 N.E.2d 334, 341 (Ill. App. Ct. 2007); *see also* Ada Cnty. Highway Dist. v. Rhythm Eng'g, LLC, No. 15-00584, 2016 U.S. Dist. LEXIS 119363, at *14–15 (D. Idaho Sept. 1, 2016); King v. Ellerlsie Corp., No. 2006-001863, 2007 Ky. App. Unpub. LEXIS 666, at *9 (Ky. Ct. App. Sept. 7, 2007); *In re* Toshiba Am. HD DVD Mktg. & Sales Practices Litig., No. 08-939, 2009 U.S. Dist. LEXIS 82833, at *52 (D.N.J. Sept. 11, 2009).

112. *See* King, 2007 Ky. App. Unpub. LEXIS 666, at *11; *see also* Oggi Trattoria & Caffe, 865 N.E.2d at 335–36; Timothy Davis, *UCC Breach of Warranty and Contract Claims: Clarifying the Distinction*, 61 BAYLOR L. REV. 783, 787 n.13 (2009) (contending that "the [implied] warranty [of merchantability] does not extend to the future performance of the delivered goods"); *see supra* notes 73, 83–93, 96–100, 103–12.

113. U.C.C. § 2-316(2) (AM. L. INST. & UNIF. L. COMM'N. 2021).

114. OWEN, s*upra* note 73, at 236; *see also* ELVY, *supra* note 6, at 161.

The federal Magnuson-Moss Warranty Act ("MMWA") can also nullify the effectiveness of any warranty disclaimer in certain transactions involving consumer products.[115] The MMWA also grants consumers a private right of action.[116] To the extent that the MMWA applies to an IoT consumer transaction, the MMWA prohibits suppliers from limiting the duration of the implied warranty of merchantability when a full warranty is provided.[117] However, the Act allows a covered entity that offers a limited warranty to limit the duration of the merchantability warranty so that it is co-extensive with the written warranty as long as the warranty's duration is reasonable and the limitation is conscionable and conspicuous.[118] Thus, under the MMWA, the duration of the implied warranty of merchantability is not tied solely to the express, limited, or full warranty that suppliers provide; rather, the duration must be reasonable, conspicuous, and not unconscionable. State law, such as Article 2 of the UCC, may be relevant in determining whether a limitation of the implied warranty is unconscionable or reasonable.[119] Although the implied warranty of merchantability should not last forever, a reasonable limitation on the duration of the implied warranty could mean that the warranty extends long enough to allow consumers to obtain the benefit of their bargain by having the ability to safely use contracted-for devices for a reasonable period of time. The average life cycle of an equivalent non-IoT product, as well as the

115. 15 U.S.C. §§ 2308(a), 2310(d); 16 C.F.R. § 700.1; *Businessperson's Guide to Federal Warranty Law*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/businesspersons-guide-federal-warranty-law [https://perma.cc/36PE-NG6W].

116. OWEN, s*upra* note 73, at 238–43.

117. 15 U.S.C. § 2308(b) ("[I]mplied warranties may be limited in duration to the duration of a written warranty of reasonable duration, if such limitation is conscionable and is set forth in clear and unmistakable language and prominently displayed on the face of the warranty."); *Businessperson's Guide to Federal Warranty Law*, *supra* note 115 ("If you offer a 'limited' written warranty, the law allows you to include a provision that restricts the duration of implied warranties to the duration of your limited warranty. . . . However, if you offer a 'full' written warranty, you cannot limit the duration of implied warranties."). State law can also contain somewhat similar provisions. *E.g.*, CAL. CIV. CODE § 1791.1(c) (West 2019); *see also* FED. TRADE COMM'N, FINAL ACTION CONCERNING REVIEW OF INTERPRETATIONS OF MAGNUSON-MOSS WARRANT ACT 27 (2015) ("[T]he MMWA preempts state warranty law unless the state law 'affords protection to consumers greater than the requirement of Magnuson-Moss.'"); Janet W. Steverson, *The Unfulfilled Promise of the Magnuson-Moss Warranty Act*, 18 LEWIS & CLARK L. REV. 155, 191–93 (2014) (suggesting that the MWMA is not intended to preempt more protective state consumer laws).

118. 15 U.S.C. § 2308(b); *Businessperson's Guide to Federal Warranty Law*, *supra* note 115. With respect to statutes of limitations and the duration of implied warranties, the FTC has noted that "[g]enerally, there is no specified duration for implied warranties under state laws. However, the state statutes of limitations for breach of either an express or an implied warranty are generally four years from date of purchase." *Businessperson's Guide to Federal Warranty Law*, *supra* note 115.

119. Popham v. Keystone RV Co., No. 15-197, 2016 U.S. Dist. LEXIS 127093, at *25–30 (N.D. Ind. Sept. 19, 2016) (relying on Illinois' version of Article § 2-302 of the UCC to determine whether a warranty limiting the duration of implied warranties is unconscionable and whether a limited remedy "fails of its essential purpose" in connection with a MMWA and breach of the merchantability warranty claim).

expectations of the reasonable buyer, could be relevant factors in such a determination.[120]

IV. CONCLUSION

IoT devices are deeply connected to the software, mobile applications, and ongoing services necessary for IoT devices to safely function and for consumers to receive the benefit of advertised device features. This Essay has highlighted the ongoing relevance of the UCC and the implied warranty of merchantability. Once a court determines that all or a portion of a transaction is subject to Article 2, the implied warranty of merchantability can play an important role in addressing potential cybersecurity and privacy-related concerns in the IoT setting. The implementation of robust cybersecurity and privacy practices is likely an important expectation of consumer buyers of IoT devices and connected services, and such practices are likely closely associated with the functionality and safety of IoT devices. The implied warranty of merchantability can be applied to ensure protection of these expectations and promote fair dealing between merchants and consumers in the IoT era.

120. ELVY, *supra* note 6, at 320–21.