"We can't allow IoT vendors to pass off all such liability to the consumer": Investigating the U.S. Legal Perspectives on Liability for IoT Product Security

Prianka Mandal*, Amit Seal Ami*, Iria Giuffrida†, Daniel Shin†, Ella Sullivan†, and Adwait Nadkarni*
*School of Computing, Data Sciences & Physics; †Law School
William & Mary, Williamsburg, VA, USA
{pmandal, aami, igiuffrida, dshin01, ecsullivan01, apnadkarni}@wm.edu

***Abstract*—As the regulatory landscape for the Internet of Things (IoT) evolves, vendors are moving towards certifying their products for security. Thus, we need to understand who is liable when certification failures result in harm, i.e., when certified products have vulnerabilities that are exploited to cause harm to users. This paper addresses the fundamental and timely question that has significant implications for vulnerability detection in certified products: *who is liable for harm resulting from vulnerabilities in certified products, and who should be so liable?* Through a qualitative analysis of contractual documents from 20 IoT vendors, this paper investigates how liability is currently defined in vendor-user contractual terms. This analysis then incorporates an expert survey of 18 legal professionals to examine their perspectives on liability within this context. Our analysis leads to 14 key findings ($\mathcal{F}_1$ – $\mathcal{F}_{14}$) that show how vendors exclude liability to the maximum extent with (sometimes unlawful) exclusions, and how the perspectives of legal experts lie in stark contrast to what we observe in contracts (which are drafted by lawyers). We distill our findings into three key themes that call for a robust and clear liability framework, creating an incentive for IoT vendors to ensure that their IoT products meet proper security and privacy standards.**

1. Introduction

As IoT products become increasingly integrated into everyday life, the growing risk of security vulnerabilities has sparked serious concerns among both consumers and governments. As a result, government bodies are pursuing policy initiatives focused on securing IoT products by enforcing security standards and requirements, such as the US Cyber Shield Act of 2021 [1], the California S.B. 327 on the security of connected devices [2], and the UK's new product security and telecommunications infrastructure regime [3]. In light of these policy initiatives, the IoT industry is responding with its own efforts to maintain IoT security compliance standards and certification in IoT products, such as the IOXT [4] and GSMA IoT [5] standards.

Prior work has studied the enforcement of security compliance/certification standards on IoT products [6], [7], particularly in instances where the products are certified by third-party certification labs. Particularly, Mandal et al. [6] demonstrate several gaps the standards and evaluation processes that result in certified products still exhibiting known and common vulnerabilities. Such certified but vulnerable IoT products may provide a false sense of security to consumers, and lead them to suffer harm resulting from exploitation of the vulnerabilities in the products. While prior work has delved into the various aspects of the security certification process, and made recommendations to make it more robust, it is clear from past evidence that compliance/certification failures are possible. What is unclear is that in the event the compliance certification process fails, i.e., when there exists a vulnerability in a certified product, and if the user suffers harm resulting from it, *who is liable*?

Establishing liability in the event of security and certification failures is critical for accountability in the IoT security certification infrastructure. That is, if it was clear from the outset that vendors and/or labs would be liable for compliance failures, and what the acceptable limitations to such liability would be in the interest of the consumer, then vendors and labs would both be motivated to do their due diligence and ensure product security. However, there has been little prior work that directly seeks to understand liability in the context of IoT product security, and security certification.

Contributions: This paper seeks to assess liability in the context of IoT product security certification through a legal perspective. Particularly, we investigate the current state of liability and exemptions through coding and a qualitative analysis of 20 "contracts", i.e., End-User License Agreement (EULA)[1] and Terms of Service (ToS) documents, from IoT vendors. We also perform an expert-survey with 18 legal experts to understand their perspectives on liability in the aftermath of security failures in IoT products. It is important to note that this work is a collaboration between law researchers (i.e., the legal team) and IoT security researchers (i.e., the security team). Hence, our coding and analysis is grounded in established legal doctrine, and also account for the technical/security nuances expressed in the documents. Our exploration of liability in the realm of IoT product security certification is guided by two key research questions

1. End-User License Agreement (EULA) can also be referred to as Terms of Service (ToS), Terms of Use, or Terms and Conditions (T&C). These terms are used interchangeably throughout the paper.

2025 IEEE Symposium on Security and Privacy (SP) | 979-8-3315-2236-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/SP61157.2025.00212

DOI 10.1109/SP61157.2025.00212

(**RQs**):

RQ$_1$: *How do IoT vendors describe liability in their contracts with users?* As we aim to understand the question of *who is liable* for IoT product failures, we focus on analyzing the contracts vendors make with users, i.e., the *End-User License Agreement (EULA)*. Several questions guide our assessment of these EULA documents. For instance, how do vendors limit or exclude liability caused by their products? What do vendors state regarding product security? How do vendors assume liability for third-party involvement? What warranties do they exclude?

RQ$_2$: *What are legal experts' perspectives on liability?* Prior work has shown that stakeholders such as developers and users have diverse perspectives on who is liable for failure in certified products [6], [7]. We aim to uncover how legal experts perceive liability in this space, as these legal practitioners are not only involved in drafting the contracts from the vendor's side, but will also defend vendors or bring legal proceedings on behalf of users in the event of a security failure resulting in harm. Therefore, we investigate legal experts' perspectives, particularly in terms of the following questions: Who do they believe is responsible for ensuring compliance standards correctly? Who would they hold liable for certified IoT product failures? Do they consider the present regulatory support for ascertaining liability sufficient?

Our coding and analysis of 20 IoT vendor contracts and the 18 expert survey responses led to 14 *key findings* ($\mathcal{F}_1$ – $\mathcal{F}_{14}$) that identify significant gaps in current liability practices in this space. For instance, we found that IoT vendors often draft liability clauses in their contracts with consumers that are too broad and, in some cases, unlawful. In most cases, even when vendors accept liability, we find restrictive clauses and ambiguous language that reduce liability to a minimal level so minor that users are unlikely to find it worth the cost and risk of pursuing litigation. Vendors also exclude warranties that consumers would not expect them to e.g., disclaim that the product would be free of vulnerabilities or viruses, or specifying that a security product such as camera should not be expected to provide security. These findings contrast with what legal experts believe, as they hold vendors liable in the event of harm resulting from IoT products, given that the vendors manufacture the product, and are able to enforce security standards. We distill these findings into three themes, which motivate a cohesive legal framework for guiding vendors, labs, and consumers on what to expect in the event of harm resulting from security failures.

Our in-depth study of End-User License Agreements (EULAs), and legal perspectives about them, directly relates to both liability enforcement in court and industry security behaviors. To elaborate, while users may not read EULAs, these are valid agreements that shape liability and security practices. If vendors systematically shift liability onto users, courts may be asked to strike out these clauses in cases of serious security failures, leading to judgments that redefine liability. Juries can also award significant damages, further influencing vendor behavior. Without clear liability rules, or awareness of liability gaps among security researchers, legal experts, and policymakers, IoT vendors may lower security standards, creating a "race to the bottom". If litigation remains the main enforcement tool, security practices will vary unpredictably, undermining consumer trust and increasing systemic risk. Our research uncovers gaps in the industry's behavior towards liability, laying the groundwork for stronger legal and policy interventions.

The rest of this paper is organized as follows. Section 2 presents the legal basis for grounding our codebook, and the background for understanding the legal perspective in this context. Section 3 describes the methodology and results of our vendor contract document analysis. Section 4 presents the survey methodology and the key findings from the expert survey. Section 5 presents the themes that are distilled from our 14 key findings. Section 6 discusses the limitations of this work. Finally, Section 7 describes the related work, and Section 8 concludes the paper.

2. Background: Liability in IoT Product Security in the Present Legal Landscape

This section describes the legal considerations and grounding that guide our codebooks for the contract and survey analysis. Particularly, the key aspects of the current liability landscape outlined next consider applicable statutory law – including key provisions of the Uniform Commercial Code—case law, and authoritative secondary sources such as legal treatises to clarify the current legal standards and obligations. This preliminary legal framework governing the liability for IoT products is shaped by contract law, tort law and, potentially, regulatory law, as shown in Figure 1. As the following section will demonstrate, this complex framework does not always support IoT users when their devices fail.

Terms of Service as Contracts: A contract is a legally enforceable promise or set of promises establishing parties' rights and obligations [8]. When a contract is formed, the law provides a remedy in case of a breach or recognizes the performance as a legally binding obligation [9]. For IoT products, the contract terms between the IoT vendor and users are contained in the terms of service or EULAs.

Courts have recognized that terms of service are a contract as long as (1) one party provides an offer of promise, (2) another party accepts the offer, and (3) there is a demonstration of consideration (something that is bargained for) between the parties.[2] Parties may demonstrate their intent to agree with the terms of the contract through words, written

2. Note, each state jurisdiction has slightly differing elements for the formation of a contract. See Shroyer v. New Cingular Wireless Servs., 498 F.3d 976, 983 ("There is no dispute that the Cingular Agreements, which refer to the Terms of Service, constitute standardized contracts."); Domer v. Menard, Inc., 116 F.4th 686, 2024 U.S. App. LEXIS 22307.

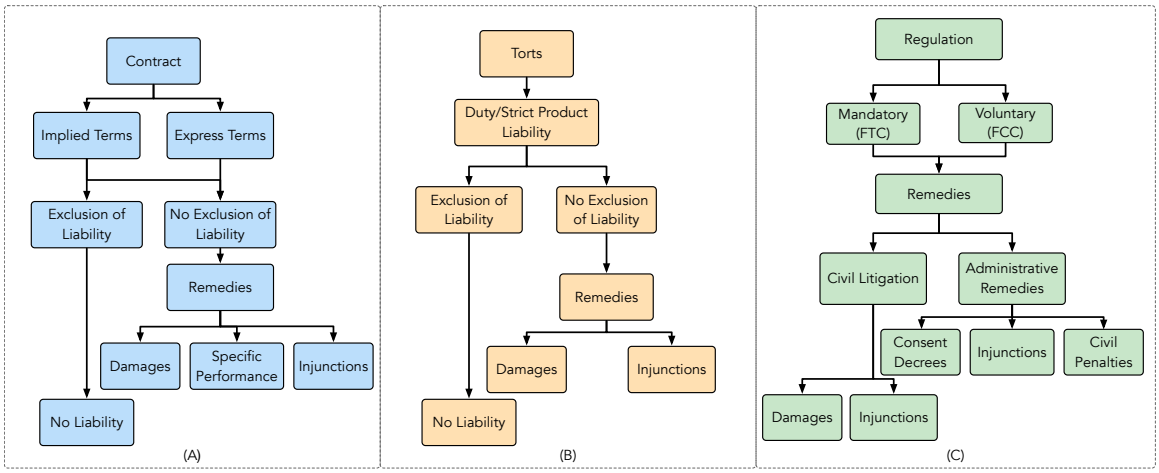

Figure 1: The overview of the current liability landscape.

or oral, and their actions,[3] and many jurisdictions do not require the agreement to be signed to be valid as long as there is a clear demonstration that both parties agreed to the contract's terms.[4]

Terms of service are examples of contracts of adhesion because they are typically prepared in a standardized form. They are presented in a "take it or leave it manner", preventing IoT users from negotiating any terms [10], [11]. Although contracts of adhesion are not unlawful and their terms are legally binding, some courts have viewed them with skepticism because users do not have a meaningful choice to assent to their terms.[5]

Warranties: Warranties are express or implied promises by a vendor that its goods are as stated or promised [12]. Express warranties are given by the vendor expressly, such as a written term in a contract, verbal undertaking, or samples in the event of a sale by sample [13]. Implied warranties arise by operation of law. In other words, they are terms implied in a contract without any parties expressly making that promise. The two main implied warranties relevant to IoT liability are (1) "fitness for a particular purpose" and (2) "merchantability". The first category refers to the vendor's responsibility to ensure that such goods fulfill a buyer's particular purpose when one is stated [14]. In the case of merchantability, the vendor must ensure that its goods are fit for their ordinary purpose of use and conform to other legal merchantability standards [15]. As explained below, parties can *disclaim* implied warranties by expressly stating in their contract that those warranties are not given [16].

Contractual Liability: When a party to a contract fails to meet its obligations, the counterpart is generally entitled to a remedy: this is what is commonly known as contractual liability [17]. The main categories of remedies that courts can grant are: (1) damages, which are monetary awards to compensate for the injury caused by the breach of contract; and (2) specific performance, which is a court-ordered directive requiring a party to perform a particular act to fulfill their contractual obligations; and (3) injunctions, which are court orders instructing a party to or refrain from certain actions [18].

Tort Liability: A tort is a civil wrong that causes a party harm for which a court will impose civil liability [19]. There are different types of torts. For the purposes of this paper, we focus on negligence and strict liability. Negligence is a tort arising from the failure of a party to behave with the level of care that a reasonable person would have used under the same circumstances. The party who suffered the harm needs to prove that the other was *at fault* [20]. On the contrary, strict liability is a form of civil liability that is imposed, in limited circumstances, regardless of fault [21]. Product liability is a form of strict liability under which product manufacturers are held responsible for harms caused by their products even if they were not at fault [22]. Typically, tort remedies comprise damages and injunctive relief. Tort damages (of which there are different categories that we are not going to examine) aim to restore the injured party to the position they were in before the harm occurred [23]. Tort law also provides for injunctive relief which is designed to restrain a party from performing certain acts or to act in a

3. Skyrise Constr. Grp., LLC v. Annex Constr., LLC, 956 F.3d 950, 956 (7th Cir. 2020) ("The intent of the parties is generally 'derived from a consideration of their words, written and oral, and their actions.'") (quoting Household Utilities, Inc. v. Andrews, 236 N.W.2d 663, 669)

4. Operating Eng'rs Local 139 Health Benefit Fund v. Gustafson Constr. Corp., 258 F.3d 645, 649 ("Nothing in the law of contracts requires that a contract, whether original or modified, must be signed to be enforceable. The contract needn't be in writing; if it is in writing, it needn't be signed, provided there's other evidence of acceptance, for example . . . by performance."); 10 Ellicott Square Court Corp. v. Mt. Valley Indem. Co., 634 F.3d 112, 124 ("[A]n unsigned contract may be enforceable, provided there is objective evidence establishing that the parties intended to be bound") (quoting Flores v. Lower E. Side Serv. Ctr., Inc., 4 N.Y.3d 363, 369).

5. Id. ("Adhesion contracts are not per se unconscionable. However, given that one party to an adhesion contract has virtually no voice in the formulation of the[] terms and language used in the contract, courts tend to view adhesive arbitration agreements with considerable skepticism, as it remains doubtful any true agreement ever existed to submit disputes to arbitration . . . .") (citations, quotes, and punctuations omitted).

particular way.

Excluding or Limiting Liability: To reduce their risks, parties can, in their contracts, exclude or limit certain contractual and tort liability [24]. While they are generally free to exclude or limit their liability, there are certain restrictions. For example, courts look suspiciously at exculpatory clauses—where a party releases the other from liability—that are too broad in their scope and can strike them down as violating public policy [25], [26]. Any clause that excludes or limits liability must be in writing, and when warranties are disclaimed, they must be specifically mentioned[6]. In general, under tort law, vendors cannot exclude through contracts their liability for their users' physical harm or death [27].

Regulatory framework for IoT: IoT vendors also face regulatory scrutiny by government agencies. Such scrutiny may come in the form of investigations that can lead to the agency taking administrative remedies against the vendors or starting litigation in civil courts. For example, the Federal Trade Commission (FTC) is empowered to monitor the consumer market and pursue enforcement action (either administratively or via civil litigation) against businesses for *unfair or deceptive acts or practices* affecting commerce [28], [29]. To pursue its statutory mission, the FTC publishes regulations covering specific contexts of business practices, including those pertaining to cybersecurity risks of consumer digital devices [30].

In another example, the Federal Communications Commission (FCC) is tasked to regulate federal communications laws, including those affecting wireless communications from IoT devices. One of FCC's major initiatives specific to IoT safety is its IoT Labeling program, called the U.S. Cyber Trust Mark [31]. This voluntary program enables participating IoT device manufacturers to comply with certain cybersecurity device standards to use the Cyber Trust Mark label on their devices [31]. Although participating in this program is voluntary, IoT device manufacturers who participate will be bound by the program requirements as long as they seek to apply the Cyber Trust Mark label on their devices [32]. If vendors subscribe to the program and fail to meet its requirements, the FCC can pursue administrative action or civil litigation.

3. User Agreement Document Analysis

To analyze how IoT vendors define liability in their contractual documents, i.e., end user licensing agreements or EULAs for their products, we performed an in-depth, qualitative analysis of such documents from 20 IoT vendors.

6. On the official comment of UCC § 2-316, the editor notes "This section is designed principally to deal with those frequent clauses in sales contracts which seek to exclude "all warranties, express or implied." It seeks to protect a buyer from unexpected and unbargained language of disclaimer by denying effect to such language when inconsistent with language of express warranty and permitting the exclusion of implied warranties only by conspicuous language or other circumstances which protect the buyer from surprise." Id.

We now describe our analysis methodology, followed by the results and findings.

3.1. Methodology

We sampled IoT vendors from a dataset developed by Manandhar et al. [33]. This dataset includes all smart home vendors that have public-facing websites, allowing us to collect EULAs. Our approach of an in-depth, qualitative, analysis required us to sample a small but relevant set of IoT vendors, even if the sample would not be representative of the IoT space (see Section 6). Thus, we first identified 10 popular and highly visible IoT vendors such as Samsung SmartThings and Wyze, and in addition, randomly sampled 10 IoT vendors from Manandhar et al.'s set. This sampling strategy allowed us to obtain impactful insights (observed in top brands), and latent insights from the random sample, making the dataset highly relevant to our analysis.

We visited each vendor's website to find the EULA that covered IoT products. Note that EULAs may not be labeled as such, i.e., in most cases, we found alternate titles for documents that covered liability for IoT products, such as "Terms & Conditions", "Terms of Service", "Terms of use", or "Legal". Table 3 in Appendix A provides the names of the 20 vendors (denoted as V1→V20), and links to their documents that we analyzed in this study.

Coding and Analysis: We used the inductive coding approach to analyze the EULA documents [34]. We randomly selected 10 documents out of the 20 to create an initial codebook via a collaborative process between authors with legal expertise (i.e., the *legal team*) and IoT security (i.e., the *security team*). To elaborate, at first, the legal team labeled the 10 documents to create an initial codebook, grounding the codes in legal theory and the liability framework described in Section 2. The security team then iterated over the same set of documents to identify additional labels, which were vetted by both teams. Once the legal and security teams converged on a codebook, two authors from the security team coded the rest of the documents using the agreed code. Note that we only considered sections and paragraphs discussing liability during the coding process. Once all the documents were coded, the coders examined the coded clauses to identify topics and themes. The coders discussed any topic or themes raised during the analysis process multiple times with the legal team to avoid any confusion and bias. We provide the codebook in Table 4 in Appendix B.

3.2. Results: User Agreement Analysis

Every agreement we analyzed includes one or more clauses addressing the limitation or exclusion of liability. In this section, we discuss the most striking clauses that vendors use to essentially *shielding themselves from all liability*.

3.2.1. Excluding Damages. The most common way vendors limit their liability is by expressly stating the categories of damages for which they will not be answerable. Our analysis reveals that the most common categories that vendors exclude are: indirect, economic, consequential, exemplary, special, incidental, punitive, lost data, corruption of data, lost profits, intangible loss, loss of privacy, diminution in value of securities, and/or property damage [35], [36]. In some cases, these clauses not only exclude categories of damages but also indicate that the vendor will not be liable even if they are aware of the possibility of such damages. For example, one vendor states that,

> *"even if any of the events or circumstances giving rise to such damages were foreseeable and even if <vendor> were advised of or should have known of the possibility of such losses or damages" — V4*

A striking finding that the analysis revealed is that in at least one case, a vendor attempted to exclude its liability for personal injury or death:

> *"Under no circumstances will <vendors> be responsible or liable to you for . . . for personal injury or death, arising from or relating to these terms of service, your account, or the mobile apps." — V9*

This exclusion is not permitted under U.S. law [27].

Finding 1 ($\mathcal{F}_1$) – Vendors go to great lengths to limit or exclude their liability. In one case, a vendor is even attempting to exclude liability for personal injury or death, which is not permitted under U.S. law.

3.2.2. Limiting Damages. As noted above, the contracts reviewed specified the categories of damages for which vendors exclude liability; however, they rarely specified the kind of damages for which vendors will accept liability. When they do so, vendors either accept liability for limited circumstances or introduce a cap limiting liability to a *de minimis* sum. Consider this case, where a contract stated that if the vendor or its employees cause any losses, the *"<vendor> shall be liable ... only insofar as intent or gross negligence can be proven"* (V12). This means that the vendor excludes its liability for loss caused by negligence and accepts liability only for gross negligence or intentional harm. This puts a high evidentiary burden on the plaintiff (e.g., *a user who suffered an actionable loss*), who must establish more than negligence.

Another approach observed in the contracts is for vendors to cap their liability amount to the sum paid by users or a specific amount. For instance, a vendor accepted liability but limited recovery by users who suffered a harm to *"the greater of the amount paid by the subscriber for . . . the service or $250.00"* (V19).

In addition to these limitations, vendors also reduce their liability exposure by introducing cumulative liability clauses. For instance, four contracts state that any vendor's liability is cumulative: *"this limitation is cumulative and will not be increased by the existence of more than one incident or claim"* (V5,V7,V9). In other words, the limitation or cap is not per harm but applies to *all* harms. Further, V13 states, *"in no event will <vendor>'s cumulative liability to you for direct damages of any kind or nature exceed one hundred dollars"*.

Another interesting finding of our analysis is that one vendor mentioned that they would be liable for,

> *"losses or damages arising out of the failure of the <vendor> to maintain proper standards of maintenance and operations" — V19*

This clause is problematic. First, it is ambiguous. The *"proper standards of maintenance"* are not defined and can, presumably, cover not only physical product maintenance but also the security compliance and certification process. However, the lack of clarity means that a user who suffered a loss may have to engage in expensive litigation to establish whether security compliance is covered by the term "proper standards of maintenance." Second, as with the contracts mentioned above, this clause enables the vendor to limit its liability to a specific amount ($250) which, on any account, is a low recovery threshold.

Finding 2 ($\mathcal{F}_2$) – Even when vendors accept some degree of liability, it is so restrictive as to be essentially *de minimis.*

3.2.3. Disclaiming Warranties. The legal system allows parties to a contract to disclaim warranties. Therefore, a vendor can protect itself from liability arising from implied warranties by including language in the contract that excludes the application of those implied warranties. This aligns with the results of our analysis. Almost all the agreements we analyzed state that the vendors provide no warranties for their products. For instance:

> *"<vendor> 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..." — V7*

One of the popular vendors who manufactures and sells smart devices like security cameras and smart locks states that their products cannot be used for security purposes, and that they are not responsible for any losses:

> *"Our Products and Services are intended to be accessed and used for noncritical, non-commercial, home-based, personal uses and not for safety, security, or time-sensitive purposes . . . <vendor> is not responsible for any damages incurred by the failure or delay of the Services or Products." — V1*

There are two noteworthy elements. First, the clause is silent as to what it means to use the device *"not for safety, security, or time-sensitive purposes"*. More importantly, the vendor here is attempting to disclaim all liability arising from the very security-sensitive features of the devices it manufactures, advertises, and sells.

Finding 3 ($\mathcal{F}_3$) – Most vendors we studied provide no warranties for their products by including language in the terms of service that exclude implied warranties. In some cases, vendors limit their liability by disclaiming the core properties of the device, e.g., that a security product (such as smart door lock, security camera) provides any security.

None of the contracts adhere to or mention compliance with any security standards that could guarantee a certain level of security in their products. Instead, vendors disclaim that their product will be *'secure'*. For example, one vendor states,

> *"<vendor> makes no warranty that the product software will be uninterrupted, free of viruses or other harmful code, timely, secure, or error-free." — V7*

Although it is reasonable not to warrant against errors or failures caused by other manufacturers or third parties, disclaiming liability for product failures arising from harmful components that a vendor could have identified and removed raises concerns. The effect of these disclaimers is that users bear the consequences of any harm caused by harmful components or a generally poor cybersecurity posture: *"You use the products and services at your own risk"* (V5).

Finding 4 ($\mathcal{F}_4$) – Vendors disclaim that the product be free from vulnerabilities, or meet any security standards, resulting in users bearing the consequences of any harm arising from a vendor's poor cybersecurity posture.

3.2.4. Ambiguity in Liability Clauses. We found several cases in which liability clauses are worded *ambiguously*, thus benefitting the vendors. Consider the case where a vendor provides a one-year warranty that their product will be free from defects. The relevant product requires batteries, and the clause recommends the *"use of only high-quality ... batteries"*. Note that this is only a recommendation, not a requirement. However, the clause proceeds to state that,

> *"the use of ... inferior-quality batteries that cause damage to your <vendor's> camera system will void the warranty." — V11*

The ambiguity arises because it is unclear what a *high- or inferior-quality* battery is, thus leaving consumers with very little guidance and bearing the risk of invalidating the warranty by selecting the "wrong" type of battery.

In another case, a vendor's limitation of liability clause is so broad, long, and difficult to understand that any user would be confused by its scope:

> *"In no event shall <vendor> or any of the <vendor> parties be liable for any indirect, special, incidental, consequential, exemplary or punitive damages of any kind (including, but not limited to, loss of revenue, income or profits, loss of use or data, loss or diminution in value of assets or securities, or damages for business interruption) arising out of or in any way related to the access or use of the site or otherwise related to these terms (including, but not limited to, any damages caused by or resulting from reliance by any user on any information obtained from <vendor>, or from mistakes, omissions, interruptions, deletions of files or emails, errors, defects, bugs, viruses, trojan horses, delays in operation or transmission or any failure of performance, whether or not resulting from acts of god, communications failure, theft, destruction or unauthorized access to <vendor>'s records, programs or systems), regardless of the form of action, whether based in contract, tort (including, but not limited to, simple negligence, whether active, passive or imputed), strict product liability or any other legal or equitable theory (even if the party has been advised of the possibility of such damages and regardless of whether such damages were foreseeable)" — V6*

The objective of this clause appears to be to exclude essentially all liability.[7]

Finding 5 ($\mathcal{F}_5$) – The use of ambiguous language in terms and conditions can lead to user's confusion. More concerning is that the terms can be so vague that they may be easily nullified by a user's actions.

3.2.5. Liability when Third-party or Sub/Independent Contractors are Involved. Our research explored the liability position when a vendor partners with a third party and the product fails. According to our document analysis, vendors excluded liability for *any damages or losses ... caused by any Third-Party Services*. For instance, one very popular vendor stated that developers may use open-source code or third-party software to further develop the code, but that the vendor does not accept any liability for losses caused by the newly developed code. The vendor *"assumes no responsibility for the use of such code and software as well as any job or consequence resulting therefrom"* (V2). Although it is not surprising that a vendor will want to insulate itself from liability arising from code developed by third parties, it leaves unanswered the question of who, if anyone, will be liable for the harm that the user has suffered.

Finding 6 ($\mathcal{F}_6$) – There is another liability gap when third parties can interact with users. Further research is needed to assess who, if anyone, is liable for the harm that the user has suffered.

3.2.6. User Notification Regarding the Agreement Revision. There is significant criticism of the "Terms and Conditions" that users are required to sign up before using

7. Downs v. Rosenthal Collins Grp., LLC, 2011 IL App (1st) 090970, 49-50 ("For an oral contract to be valid and enforceable, its terms must be definite and consistent. When it appears that the language used or the terms proposed are understood differently by the parties, there is no meeting of the minds and no contract exists.") (internal citations omitted); Express Indus. & Terminal Corp. v. New York State Dept. of Transp., 693 N.Y.S.2d 857, 860 (1999) (finding that the contract's terms were so vague that there was no way to determine what the parties' actually agreed to).

the services or products because they are, essentially, contracts of adhesion. Users cannot negotiate terms; they can either agree to terms or not use the service or device. On the contrary, vendors can revise any terms at any time and, in most circumstances, they are not even obligated to inform users. That is, the responsibility of checking and reviewing the updated terms is left to users:

> *"we may change these Terms in our sole discretion. We reserve the right to make these changes without notice ... You are responsible for regularly reviewing these Terms" — V14*

It seems striking that privacy regulations emphasize the importance of transparency and communication, thus requiring notifications of changes in privacy protections. On the contrary, changes to users' rights to seek redress for losses caused by the vendors require no notification.

Finding 7 ($\mathcal{F}_7$) – Vendors may revise the agreement at any time and without notice. This shifts the burden of reviewing the terms and conditions periodically to the users, if they are to understand their rights and seek redress for losses.

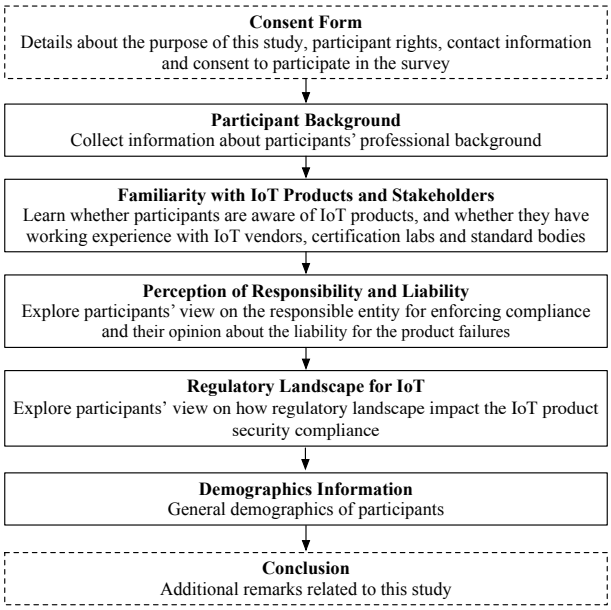

Figure 2: Overview of the survey design.

4. Survey of Legal Experts

We use an expert survey followed by qualitative analysis to answer $\mathbf{RQ}_2$, i.e., to help us understand *how legal experts view the liability for IoT security failures*. This section describes the survey and analysis methodology, followed by the results and findings.

4.1. Survey Methodology

We conducted a survey with 18 legal experts, i.e., lawyers well versed with U.S. law, recruited from our professional networks. This section describes the survey design, participant recruitment process, ethical considerations, and data analysis.

4.1.1. Survey Design. The security and law researchers conducting this study project collaboratively designed the survey, with the goal of drafting clear questions for our target expert population, and avoiding any potential confusion or bias. The resultant survey consists of 38 questions, with a mix of multiple-choice questions, Likert scale questions, and open-ended questions. Among these, certain questions are conditional, e.g., if the participants confirmed familiarity with the U.S. Cyber Trust Mark, we asked more questions related to this program), while others are optional (e.g., demographic questions). As shown in Figure 2, our survey is organized as follows (see Appendix C for the survey instrument):

Section-A. Background Information: We asked questions related to the participants' backgrounds, including employment status, years of professional experience, and the subfield in which they work within the legal profession.

Section-B. Familiarity with IoT Products and Entities involved in IoT Security Certification: We asked participants if they were familiar with IoT devices and IoT companion apps. Next, participants were asked if they had experience working with IoT vendors, certification labs, and/or standard bodies.

Section-C. Perceptions regarding Liability in the Event of IoT Security Failures: This section aimed to gain participants' perceptions regarding compliance enforcement and liability for vulnerable, certified products. We presented two hypothetical scenarios inspired by a prior study [6] and asked the participants to rate the severity of those scenarios (see Section 4.2.2 for a description of the scenarios). Next, we asked the participants' opinions about which key stakeholders (IoT vendors, certification labs, standard bodies, users) (see Appendix C for definitions of each stakeholder) they think are responsible for enforcing the correct IoT compliance standards. After learning their perspectives on compliance enforcement, the participants were asked which key stakeholders they think should be liable for the security failures in certified IoT products.

Section-D. Regulatory Landscape: We asked questions regarding the participants' familiarity with the regulatory landscape for IoT products. More specifically, we asked if the participants were aware of the IoT Cybersecurity Labeling Program [37] by the FTC and their opinions about the impacts of such a program. We also asked their views on whether the FTC's enforcement actions have any impact on IoT vendors' perceptions of security compliance.

Section-E. Demographic Information: We asked participants to provide demographic information (particularly age, gender, and education). These questions were optional.

Before releasing the survey to our target participants,

we conducted a pilot study with five participants from our professional network: one expert in security research, two legal experts, and two graduate students. Based on the feedback from the pilot study, we revised the survey until no issues were raised. We excluded the responses from our pilot study data from our analysis to avoid biases.

4.1.2. Participant Recruitment. As our goal was to obtain expert opinion from legal practitioners, we focused on recruiting few participants whose responses would be reliable in terms of quality, rather than a mass survey focused on obtaining a large number of responses. Thus, we invited legal practitioners of law in the U.S. from our professional networks to participate in the survey. Each participant was sent a personalized email. We received 18 complete responses.

4.1.3. Ethical Considerations. Our survey was approved by our Institutional Review Board (IRB). Participants were informed of the goal of the study before participating in the survey. Participants were also informed that there is no penalty if they wanted to withdraw from the study at any time. Each participant provided consent to participate willingly, including the consent to disclose anonymized survey responses and quotes. However, if participants indicated that they did not want their responses to be used as quotes in the paper, we respected their choice and did not include them. Finally, participants were not compensated, as any form of payment would be construed as seeking professional/legal advice, and prevent participants from expressing their unbiased opinion.

4.1.4. Data Analysis. We used the inductive coding approach to derive codes from open-ended question response data [34]. For each open-ended question, two coders coded all the responses and created the codebook. Therefore, we did not rely on inter-rater reliability measures [38]. After creating the codebook and identifying initial themes, the coders refined the identified themes following discussions with the team. The coders discussed any patterns or themes raised during the analysis process multiple times with the law research team to avoid any confusion and bias. We present the results of our analysis in Section 4.2.

4.2. Results: Perspectives of Legal Experts

This section describes the results from our analysis of the survey responses. Since the participants are 18 expert legal professionals and our analysis is mostly qualitative in nature, we did not interpret the results using absolute quantitative terms. However, we followed a standard approach, used in prior work [39], [40], of using qualifiers such as *few, many*, and *most* to describe proportions (as shown in Figure 3). In this section, we first describe our participants' background and familiarity with IoT products. Next, we discuss the participants' perceptions regarding IoT compliance enforcement and their opinions on liability in the event of security and privacy failures in IoT products. Finally, we present the

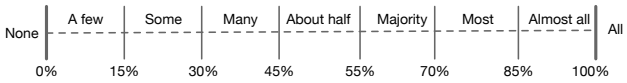

Figure 3: The details of qualifiers and respective percentages that were used to describe the survey results.

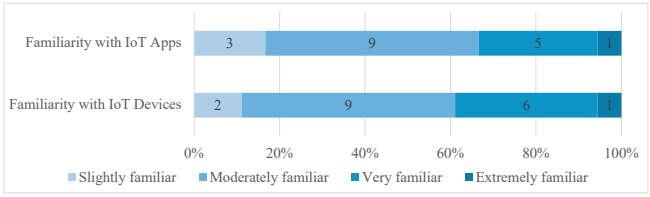

Figure 4: Participants familiarity with IoT devices and IoT apps

practitioners' opinions on the regulatory landscape related to the IoT ecosystem.

4.2.1. Overview of participants. The 18 legal practitioners are experts in diverse domains. While some are privacy and cybersecurity practitioners, others are experts in compliance, telecommunications, technology, media, intellectual property, corporate law, national security, and state government. All participants are currently practicing law full-time. Table 1 provides our participants' background information and Table 2 provides aggregated demographic information.

All participants are familiar with IoT products (i.e., IoT devices and IoT companion apps), as shown in Figure 4. Almost all are at least *moderately* familiar with IoT devices and IoT companion apps. This indicates that while our participants are legal experts, they are also familiar with the study topic. Further, three participants have working experience with IoT vendors and standard bodies (e.g., the National Institute of Standards and Technology (NIST) [41]), and one of them also has experience working with certification labs.

4.2.2. Perceptions on IoT Product Security Certification. To understand how legal practitioners perceive IoT security compliance enforcement/certification, we presented a scenario where a certified IoT product has a vulnerability that allows an attacker to steal sensitive audio/video data while the device communicates with its companion app. Almost all the participants expressed that this scenario is critical/high in severity, with few participants identifying it as medium severity. While asking the participants' legal perspectives on the liability in the event of security and privacy failures in IoT products, we presented two variations of this scenario: (i) the vulnerability in the IoT products is within the scope of the IoT security standards that certification labs followed when certifying the IoT products (S1), and (ii) the vulnerability in the IoT products is outside the scope of the IoT security standards (S2). The results presented in this section are based on these two scenarios.

We now describe the participants' perspectives and their rationale on who is responsible for enforcing security com-

TABLE 1: Overview of the participants: participant ID, field of expertise (self-reported by the participants) and years of professional experience. We used a range for describing the years of professional experience instead of an exact number.

Participant ID	Field of Expertise	Years of Experience
P1	Compliance investigations in house	5-15 years
P2	Cybersecurity and Data Privacy	<5 years
P3	Banking and Finance	<5 years
P4	Technology, State Government, Privacy, Cybersecurity	5-15 years
P5	Corporate Litigation	<5 years
P6	Litigation	<5 years
P7	Intellectual property	<5 years
P8	Law Firm	<5 years
P9	Cybersecurity & Privacy	5-10 years
P10	Securities Law	15+ years
P11	Financial Regulation	5-15 years
P12	Privacy & Cybersecurity	5-15 years
P13	Intellectual property litigation	<5 years
P14	Telecommunications, technology, and media	<5 years
P15	Private sector privacy & AI regulatory compliance	5-10 years
P16	Litigation	<5 years
P17	Commercial Litigation	15+ years
P18	Cyber, national security, corporate	15+ years

TABLE 2: Participants' Demographic Information. Two participants chose not to answer the demographic questions.

Gender(%)		Age(%)		Education(%)	
Male	55.56	18-29 years old	22.22	Doctorate	55.56
Female	33.33	30-39 years old	27.78	Masters	5.56
		40-49 years old	27.78	Juris Doctor	11.11
				Professional Degree	16.67

pliance for IoT products in the event of these two scenarios.

IoT vendors are the most responsible by default: Almost all participants held IoT vendors most responsible for ensuring security compliance regardless of the scenarios. The key reason is that they manufactured and sold the relevant product, and hence, they have the utmost responsibility to keep their products up-to-date and free from vulnerabilities. As P5 said:

> *"IoT Vendor should be responsible because it is their product..." — P5*

As IoT vendors are responsible for the quality of their products and ensuring that their products meet all necessary criteria before going to market, they need to choose the certification lab rigorously, as one of our participants explained:

> *"I also view an IoT vendor as responsible for (if applicable) which standards body and certification lab are selected. A decision to reach a lower threshold or test less stringently is a question of responsibility, although not necessarily an absolute question." — P13*

It is important to consider these perspectives in conjunction with the fact that vendors may resort to *forum shopping* [42], i.e., select labs that offer quick/cheap certification with inadequate testing, due to time and budget constraints [7]. That is, when vendors indulge in such efforts to sidestep adequate security practices, legal experts may hold them ultimately responsible.

Finding 8 ($\mathcal{F}_8$) – Practitioners consider IoT vendors as primarily responsible for enforcing security compliance as they manufacture/sell the products, and are thus responsible for preventing vulnerabilities.

Certification labs are responsible if the vulnerability is within the scope of the security standards: When vulnerabilities were found in the certified products, the majority of our participants mentioned that certification labs are also responsible for ensuring security compliance. Since certification labs evaluate and certify the products, they should be responsible for ensuring that those products do not have vulnerabilities. P14 noted that,

> *"The certification lab is responsible for certifying only compliant products, so a product with such a vulnerability should not have received certification." — P14*

Participants also expressed that the certification labs should continuously improve to keep their bar high for detecting vulnerabilities and ensuring proper security compliance. On the other hand, even though a vulnerability is within the scope of the standard, one participant argued that labs may not be responsible as they may not have full access to the software/code of the relevant IoT products. Instead, they *"may be relying on vendor representations when making their determination to issue a certification, and may lack the authority to look at proprietary source code. (P12)"*

If a vulnerability is outside the scope of the certification standards, only few participants expressed that certification labs are responsible for ensuring security compliance. One suggested the certification labs must engage in *"continuous adjustment to new needs and threats. (P5)"*.

Finding 9 ($\mathcal{F}_9$) – As per legal practitioners, certification labs should be responsible for ensuring that IoT products meet all the criteria of the standards and do not have vulnerabilities that fall under the scope of the standard.

New security threats may *(not)* also make standard bodies responsible: We found contrasting sentiments for the responsibility of standard bodies with respect to the discovery of new security threats. One group noted that since security is evolving and new threats are discovered regularly, the standard bodies should be held accountable for changing the standards to adapt to the new threats.

> *"This is a very complex market that needs continuous adjustment to new needs and threats. All three (IoT*

vendor, certification lab and standard body) should be able to keep up with ongoing changes." — P5

On the contrary, the other group's view is that new threats are discovered frequently, and standard bodies cannot be expected to update the standard criteria every time something new is discovered; therefore, the standard bodies should not be responsible. As P8 expressed,

"...this is nearly impossible to do, especially as quickly as tech is evolving." — P8

It is interesting that both groups implicitly assumed that standard bodies would have appropriately accounted for all known vulnerabilities in the standards. This may not be accurate, as prior work has found that the criteria of IoT security standards can be incomplete, overly broad, and have loopholes [6].

4.2.3. Perception of Liability. This section describes the legal experts' opinions regarding who is and who should be liable in the event of security failures in IoT products.

IoT vendors are (*should be*) liable by default: Most participants agreed that when a vulnerability is discovered in a certified IoT device, regardless of whether it falls within (S1) or outside (S2) the scope of security standards, IoT vendors should be the primary party held liable for the security failures in their IoT products. The rationale employed by the participants is connected to $\mathcal{F}_7$, i.e., as IoT vendors are responsible for developing products and and ensuring their security, they should also be held liable for any harm or loss resulting from a vulnerability in the product. That is, as P12 states,

"Only the IoT Vendor has the ability to design and implement security controls and test for vulnerabilities." — P12

However, one of our participants (P12) raises an important question: when IoT vendors deliver IoT products *in partnership with another company*, *who is liable? (P12)*. We find that the liability can be influenced by the *source of the vulnerability*, as we discuss in detail in Section 3.2.5. That is, IoT vendors may be inclined to disclaim all the liability in the event of third party's involvement.

Finding 10 ($\mathcal{F}_{10}$) **–** Practitioners view IoT vendors as entirely liable for any harm that occurs because of a vulnerability in IoT products.

The liability of certification labs depends on the contracts with their vendors and the *nature of the vulnerability*: We observe that the participants would hold certification labs liable depending on the *nature of the vulnerability*, i.e., whether the vulnerability is known and within the scope of security standards or is unknown and outside the scope of the security standards. To elaborate, the majority of our participants mentioned that certification labs should be liable for a vulnerability that is known and within the scope of security standards (S1). Most participants expressed that certification labs should not be liable for a vulnerability that is unknown and outside the scope of the security standards (S2).

In general, participants mentioned that certification labs should be liable for any negligence in their assessment.

"The responsible parties (IoT Vendor, Certification Lab) should be jointly and severally liable for harm that resulted from what was presumably negligent development, certification, and marketing of a noncompliant device" — P14

Finding 11 ($\mathcal{F}_{11}$) **–** While practitioners would hold certification labs liable for negligence, their general view is that liability of certification labs depends on the contract between the labs and IoT vendors. That is, labs would not be held liable for vulnerabilities that are outside of their scope of work, given the standards they follow.

Further, some participants expressed the view that certification labs are *"unlikely to be directly liable to the user"*, rather they are liable to the IoT vendors.

"The Certification Lab should be liable to the IoT Vendor depending upon the agreement, its conduct, and the nature of the failure/vulnerability" — P10

The majority of the participants did not change their view on who should be liable when presented with a hypothetical contract: *if it is established that the contract between the IoT Vendor and the Certification Lab contains a clause that* (i) *limits the Certification Lab's liability to the IoT Vendor to a low sum of money, and* (ii) *excludes any consequential damages to the IoT Vendor and third parties, such as users.* Participants argued that if certification were mandatory, this clause would not be enforceable. In that case, certification labs should be liable for cybersecurity incidents arising from certified IoT devices when the IoT vendors *must* certify their IoT products. As P16 states,

"Exculpatory clauses such as this should not be permissible in a situation where the vendor does not have an alternative option other than not to get a certification–it should be akin to fiduciary duty exculpatory clauses where they are void on their face." — P16

Finding 12 ($\mathcal{F}_{12}$) **–** In the event that certification is *mandatory* for vendors, legal practitioners view exculpatory clauses in contracts between vendors and certification labs as unenforceable and void.

Finally, participants suggested that (i) certification labs that do not engage in meaningful assessment should be held liable for harm caused by known vulnerabilities and (ii) while certification labs need to assess and certify IoT products that comply with the security standards, they also should *name & shame* products that fail the assessment. As described by P13:

"We do not want a liability scheme which will preclude the existence of a reliable independent lab who will not only rate IoT Devices, but also identify which

IoT Devices fail to meet standards — not just publish those that pass the standard tests. But there should be liability where the certification lab has rubber stamped a known vulnerability" — P13

Users are victims, and should not suffer the loss without redress: In the event of security failures in IoT products, users will likely suffer the harm caused by low/inadequate IoT cybersecurity protections. The other entities, especially IoT vendors, should be liable to users.

"The vendor is potentially liable to the user for harms suffered" — P12

However, suppose the user is using the IoT device *"in a manner that was inconsistent with the Terms of Service (P12)"*. In that case, some participants thought that the user should bear fully the harm caused by any security failures arising from their actions. If users have created a security vulnerability, they should suffer the consequences. Few participants also explained that users may carry some liability if they contributed to the harm, depending on their jurisdictions.

"Under the tort laws of certain states, the user may have some liability." — P4

4.2.4. Perception of the Regulatory Landscape.

This section describes the participants' opinions regarding two regulatory landscapes: (i) FCC's US Trust Mark and (ii) FTC's enforcement actions. In the post-Chevron reality, this landscape may have changed.[8] However, we wanted to assess whether legal experts considered that a regulatory framework would have a positive impact on security compliance.

The impacts of the U.S. Trust Mark: Some participants confirmed familiarity with the IoT Cybersecurity Labeling Program, *U.S. Cyber Trust Mark* and highlighted the effects of this program. Participants expressed that such programs encourage establishing at least minimum security standards for IoT products leading to more trusted products on the market. That is, products carrying the Trust Mark, will help consumers make informed decisions [40], [44], [45]. P14 noted that,

"it will be helpful to mark devices with some indication of their security to help educate consumers and help them make informed decisions." — P14

Prior studies also found similar sentiments among consumers who are willing to buy products with more security [46].

However, participants noted that acquiring the mark can be costly. Higher costs are often passed on to the consumers, thus making the products more expensive. Participants also mentioned that following certain standards may have the *"potential to leave significant number of vulnerabilities unaddressed (P4)"* in products. Compliance standards can be treated as a checklist [47] which may give flexibility to developers and testers, but may encourage them not to look at other possible vulnerabilities. Therefore, consumers may get a *false sense of security* when buying those certified products.

"Consumers will just look for the mark and not do further research into the best and most secure products." — P14

Finally, participants mentioned three factors that may determine the success of the program: (i) quality of certification process, (ii) adoption rate by vendors, and (iii) consumer knowledge.

Finding 13 ($\mathcal{F}_{13}$) **–** Participants consider initiatives like the U.S. Cyber Trust Mark as a net positive, although their success also depends on the quality of the certification process and adoption by vendors. However, such initiatives may also backfire by making users prone to a false sense of security, as they abandon all due diligence and solely trust the "mark".

The impact of risk of enforcement on IoT vendors: Considering the Federal Trade Commission (FTC)'s enforcement actions pertaining to consumer IoT devices, almost all participants noted that the risk of enforcement actions has an impact on how IoT vendors approach security compliance. Vendors want to avoid being at the receiving end of any enforcement action for two main reasons: (1) market reputation and (2) cost linked to defending the action.

"When there are consequences, corporations tend to be more careful with the quality of their products." — P16

Further, participants hoped that regulatory enforcement would encourage IoT vendors to choose the correct security compliance and expert team.

"It seems regulations could promote vendors being more diligent about security compliance and being sure the entities they hire are doing a good job." — P8

However, while it may help vendors to focus more on security compliance and the quality of the product, participants expressed that ensuring compliance can also not be enough to ensure proper security, as vendors only focus on fulfilling the criteria of the compliance standards.

"Similar to my experience in financial regulation, companies may approach security compliance too narrowly, as it focuses almost exclusively on what regulators or standards agencies prescribe." — P11

Finding 14 ($\mathcal{F}_{14}$) **–** Participants believe that regulatory enforcement may influence IoT vendors to ensure the quality of the products with high-security standards because of the market reputation and the cost associated with defending the enforcement. However, they may also make vendors focus solely on compliance requirements rather than security, thereby reducing the outcome to solely the satisfaction of compliance criteria.

8. The so-called *Chevron* doctrine was overruled by the Supreme Court in June 2024, in *Loper Bright Enterprises v. Raimondo*, 603 U.S.— (2024). Since 1984, this had been "the leading doctrine on how to divide authority between agencies and courts in determining statutory meaning." [43].

5. Discussion

This section distills our 14 findings into 3 key themes (Section 5.1→5.3) that capture critical gaps that must be addressed for enforceable and effective liability-based guardrails for IoT products. Particularly, we observe that inadequate EULAs can create significant gaps in determining liability, allowing vendors to avoid liability even when they should be liable as per the perspective of legal experts. This results in consumers being unable to redress the losses they suffered as a consequence of the failure of certified IoT products, highlighting the necessity for a cohesive liability framework for IoT (Section 5.4).

5.1. Contracts with the user need significant improvement and scrutiny

It is not surprising that these contracts are written in a way that benefits the vendor in the event of a security/safety failure and loss. However, what is surprising is the extent to which vendors exempt themselves from liability, which, without scrutiny from policymakers and consumers, would lead to users bearing the consequences of any and all harm arising from the vendor's negligence or gaps in their cybersecurity posture.

To elaborate, we find that even popular vendors may exclude liability for personal injury and death, an exemption that is not even permitted under U.S. law ($\mathcal{F}_1$). And even when vendors do accept some liability, the phrasing in the contract makes it so restrictive that the liability is essentially too trivial to be ligigated ($\mathcal{F}_2$). We also found vendors to exempt any and all warranties associated with security ($\mathcal{F}_4$), e.g., meeting established security standards, being free of "viruses or harmful code", even when security was the core and advertised purpose of their device ($\mathcal{F}_3$). Add to this that the ambiguous wording often allows the vendor to escape liability based on certain user actions ($\mathcal{F}_5$), or change the terms without informing the user ($\mathcal{F}_7$). This reveals a highly unaccountable landscape, where vendors are not even required to do the bare minimum to prevent users from harm. That is, when a EULA/TOS representing security cameras and door locks states that the devices cannot be used for "security, safety", we can only reach one conclusion: that *such contracts offer negligible protections to the user, and need significant public scrutiny to motivate any improvement.*

Such scrutiny need not come directly from consumers, as prior work has shown that users are highly unwilling to read such contracts, and often accept ToS documents without reading them [48]. Instead, the scrutiny should come from policymakers and regulators, i.e., standards such as the U.S. Cyber Trust Mark should also regulate the extent to which vendors may exempt themselves from warranties and liability, and clearly articulate exemptions that would be unconscionable, keeping the interest of consumers and the security of the IoT ecosystem in mind. The findings from this study will contribute to laying the groundwork for such guidance.

5.2. There is a gap between how contracts express liability, and who legal experts deem liable

As discussed previously, EULAs and ToSs appear to be written primarily to afford vendors significant exemptions in terms of liability and warranties. In contrast, from our survey we observe that legal experts hold vendors as primarily liable under the same situations that the EULAs would exempt, i.e., in the event of harm resulting from vulnerabilities in IoT products ($\mathcal{F}_{10}$). The rationale for this is simple: as vendors manufacture and sell the products, they are also primarily responsible for enforcing standards and preventing vulnerabilities ($\mathcal{F}_8$). Thus, there exists a clear gap in how liability is expressed in contracts presented by vendors, and how legal experts perceive liability.

There may be an explanation for this gap that is rooted in the context in which legal experts participated in our survey, versus the professional context in which they are hired by vendors for drafting EULA and ToS documents. That is, when hired by the vendor, legal experts have a duty to act in their client's best interest and, therefore, develop a contract that gives their client maximum leeway if liability were to arise. However, the responses to our survey were voluntary (and not paid professional service) in the interest of improving our understanding of liability in the IoT context and the state of IoT security in general. Thus, participants discussed who they believed courts would hold liable in the event of harm ($\mathcal{F}_{10}$, $\mathcal{F}_{11}$, $\mathcal{F}_{12}$), or who should ideally be considered responsible for ensuring product security ($\mathcal{F}_8$, $\mathcal{F}_9$).

5.3. Liability in IoT is unclear in the existing compliance certification ecosystem, and consumers may be unable to redress the losses

Although the legal experts from our study believe the IoT vendors are the primary party responsible for ensuring security standards for their products ($\mathcal{F}_8$), and are liable in the event of harm ($\mathcal{F}_{10}$), our findings reveal that liability can not be easily attributed to vendors. This is due to key aspects observed in the EULAs/ToSs, such as severe exclusions of liability ($\mathcal{F}_1$, $\mathcal{F}_2$) and warranties ($\mathcal{F}_3$, $\mathcal{F}_4$), and ambiguous clauses regarding what damages are considered and what actions of the user may void the warranties ($\mathcal{F}_5$). That is, while the legal experts from our study believe vendors should be held liable, given the EULAs, it is unclear if they would ever be.

In terms of attributing liability to certification labs, the situation is just as nuanced. For instance, most legal practitioners agree that labs are not responsible for anything that falls outside their scope of work ($\mathcal{F}_9$). Defining the scope of work is not straightforward ($\mathcal{F}_{11}$), and dependent on both what the security standard covers, as well as limiting factors such as the contract between the vendor and the

lab and the presence of proprietary code that may make it harder for the lab to effectively test the product. That said, if certification is mandatory, then practitioners also viewed exculpatory clauses that would exempt the lab from liability as void under U.S. law.

Finally, when it comes to third party involvement in the development of products, contracts from vendors disclaim liability for any damages caused by third parties ($\mathcal{F}_6$). This observation was also found in prior work [7] where IoT practitioners blame third parties for vulnerabilities in their code, and disclaim any responsibility toward the same.

To summarize, liability is unclear even if there is harm to the user, motivating the need for a cohesive legal framework for guiding vendors, labs, and consumers on what to expect in the event of harm resulting from security failures. A clearly laid out liability framework, coupled with regulatory enforcement such as by the FTC, FCC or other competent regulator, may be necessary and sufficient to incentivize IoT vendors to follow security best-practices for their products ($\mathcal{F}_{14}$). However, the scope of enforcement for agencies like the FTC may have changed in the post-Chevron-doctrine landscape.

5.4. Establishing the foundation for future liability framework research

Our study examined U.S. legal perspectives on IoT security liability, revealing a significant gap. IoT vendors heavily limit liability, yet legal experts overwhelmingly agree that vendors should be responsible for security failures. Without regulatory intervention, litigation will be the primary mechanism for addressing liability, making our contribution especially timely.

We show that broad liability disclaimers ($\mathcal{F}_1$–$\mathcal{F}_7$) influence vendor security practices, diverging from legal experts' views on accountability ($\mathcal{F}_{10}$–$\mathcal{F}_{12}$). Three key forces drive vendor behavior and security practices, and the potential liability framework:

1. Legal Accountability: Just as product liability law prevents manufacturers from disclaiming responsibility for certain defects, IoT vendors should not be able to escape liability for security failures caused by negligence or non-compliance. Vendors frequently draft overly broad disclaimers ($\mathcal{F}_1$-$\mathcal{F}_3$), some legally questionable. Courts can clarify liability limits by invalidating these clauses ($\mathcal{F}_{10}$–$\mathcal{F}_{12}$).

2. Market and Contractual Transparency: IoT contracts often obscure liability disclaimers in complex legal language ($\mathcal{F}_5$), making vendor obligations unclear. Standardized, plain-language disclosures—similar to consumer finance laws—would enhance transparency and enable informed decision-making. In a competitive market, clear and fair liability terms may also strengthen consumer trust.

3. Litigation as the Primary Driver of Change: With little near-term regulatory oversight, litigation will shape vendor behavior ($\mathcal{F}_{14}$). Courts can strike down unfair contract terms under doctrines like unconscionability and public policy, and class action lawsuits may deter excessive liability waivers ($\mathcal{F}_6$). If litigation is the main enforcement tool, security practices will vary unpredictably, undermining consumer trust and increasing systemic risk.

6. Limitations

This work is the first to examine the current state of liability for IoT products from a legal perspective. The contributions of this paper should be examined in the light of the following limitations:

1. U.S. Context only: Our study focused on the liability for IoT products from the U.S. legal perspective. Different countries have different regulatory landscapes for IoT products, and exploring liability from other regions' legal perspectives is out of the scope of this paper.

2. Sample Size: While our document sample size (n=20) may seem small, sample size is not considered as a primary factor affecting quality of data in qualitative research [49], [50] Further, during our qualitative analysis of documents, we repeatedly found the same topics in the documents as we continued, indicating that we reached data saturation. Our key findings from document analysis revealed significant ambiguities and inconsistencies in the IoT vendors' EULA documents. Finally, our methodology and codebook are sufficiently repeatable and grounded in legal theory and precedents (see Section 2) to be applied to IoT vendors' EULA documents and other software product vendors' EULA documents.

3. Survey Limitations: We conducted the survey with a small number of legal experts (n=18) and reported the findings based on qualitative analysis. While the number of participant is small, this is an expert study and the sample size is comparable to other expert studies published in the security and privacy venues [44], [51]. However, while the limited number of participants means that our results may not be generalizable to a larger population, the expertise and diverse professional backgrounds of the participants indicated that the survey can be viewed as reliable.

7. Related Work

Our work investigates the current IoT vendors' liability practices for security failures. This section briefly overviews prior research work related to and complementary to ours.

Security and Privacy of IoT Products: Significant research work has been done focusing on security vulnerabilities in IoT products (e.g., [52], [53], [54]). For instance, prior works focused on the security analysis of Mobile-IoT apps [55], [56], [57], [58], [59], demonstrating that IoT apps are vulnerable, and user data can be compromised. Our work investigates the liability of entities involved with these types of security failures in IoT. Further, several researchers focused on analyzing the privacy disclosures of IoT products in the form of privacy policies [33], [60]. For instance, Manandhar *et al.* examined the current state

of smart home privacy policies [33] and found significant inconsistencies in privacy policies. However, privacy policy contains information related to how vendors protect the user data. On the other hand, Terms of Services (ToS) are contracts between vendors and users about the product use and liability. Therefore, our work focuses on examining the Terms of Services documents.

Product Security Compliance and Certification for IoT: Prior work focused on IoT product security in terms of compliance standards and security labels. Similar to the security compliance/certification initiatives [37], [61], [62], [63], researchers also introduced 'security labels' for IoT products [44], [45], [64], [65]. For instance, Emami-Naeini *et al.* designed a usable and informative IoT security and privacy label to help users make informed decisions [64]. While these works focus on the certification mark and security labels for IoT products, Mandal *et al.* studied the current state of the IoT certification model in practice [6]. They showed that certified Mobile-IoT apps can have vulnerabilities, and the consumers hold developers (hence the vendors) of those apps liable for those vulnerabilities [6]. On the other hand, IoT practitioners believed that certification labs should be liable for the vulnerabilities found in certified products [7]. These works only discuss liability from consumers' and industry perspectives, while our work aims to discuss the liability from legal perspectives by analyzing Terms of Services documents and conducting a survey with legal experts.

Consumer Behavior towards IoT Security: Finally, there is research work that investigates consumers' expectations and behavior towards the security and privacy of IoT products and their opinions on responsible entities for ensuring security and privacy in IoT products(e.g., [66], [67], [68], [69], [70], [71]). For instance, Haney *et al.* interviewed 40 smart home adopters to investigate participants' expectations about responsibility for ensuring the security and privacy of IoT devices, and showed that participants expect users, manufacturers, and the government to share responsibilities of the security and privacy of IoT devices [66]. Further, Kustosch *et al.* surveyed 862 consumers to investigate their expectations around the responsibilities of security and privacy events that would and should be handled [67]. We deviate from these works as we (1) study the liability of IoT product security failures by (2) focusing on the U.S. legal perspectives of the liabilities.

8. Conclusion

This paper provides a comprehensive understanding of the current state of liability and what should be, in terms of IoT product failures. It presents a qualitative analysis of EULA documents from 20 IoT vendors, and an expert study with 18 legal professionals, that together lead to 14 key findings. The findings from the document analysis demonstrate that liability clauses can be ambiguous and too broad, often leading to user confusion and potentially benefitting vendors. However, survey results highlight that vendors should be the primary responsible entity for ensuring security compliance standards in their products, and they should assume liability for any security failures. Further, the study emphasizes the need for regulatory enforcement to motivate IoT vendors toward maintaining proper compliance security standards for their products. To summarize, for vulnerability research to be fruitful, the legal consequences of vulnerabilities must be clearly understood. Legal considerations are central to the future of vulnerability research, and this work fosters a much needed and timely conversation on liability for IoT security failures, providing a foundation for continued interdisciplinary exploration.

Acknowledgments

The authors would like to thank the shepherd, and the anonymous reviewers for their constructive feedback on the paper. The authors thank Shelby Conley and Taylor S. Cannatelli from William & Mary Law School for their help in the preliminary analysis necessary for the study. The authors have been supported in part by the NSF-2237012 and NSF-2132281 grants. Any opinions, findings, and conclusions expressed herein are the authors' and do not reflect those of the sponsors.

References

[1] United States Senate, "S.965 - cyber shield act of 2021," https://www.congress.gov/bill/117th-congress/senate-bill/965, 2021.

[2] California Legislature, "Sb-327 information privacy: connected devices." https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327, 2020.

[3] Viscount Camrose, "The uk product security and telecommunications infrastructure (product security) regime," https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime, 2024.

[4] ioXt Alliance, "ioXt: The Global Standard for IoT Security," https://www.ioxtalliance.org/, 2021.

[5] GSMA, "GSMA | IoT Security Assessment | Internet of Things," https://www.gsma.com/iot/iot-security-assessment/, Accessed July 2021.

[6] P. Mandal, A. S. Ami, V. Olaiya, S. H. Razmjo, and A. Nadkarni, ""Belt and suspenders" or "just red tape"?: Investigating Early Artifacts and User Perceptions of IoT App Security Certification," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 4927–4944. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/mandal

[7] P. Mandal and A. Nadkarni, "'We can't change it overnight': Understanding Industry Perspectives on IoT Product Security Compliance and Certification," in *Proceedings of the 46th IEEE Symposium on Security and Privacy*, May 2025.

[8] B. A. Garner, Ed., *Contract, BLACK'S LAW DICTIONARY (11th ed.)*, 2019.

[9] *RESTATEMENT (SECOND) OF CONTRACTS § 1.* AM. LAW INST., 1981.

[10] *17A AM. JUR. 2D CONTRACTS §274.*

[11] *Damico v. Lennar Carolinas, LLC, 437 S.C. 596, 613, 879 S.E.2d 746, 756*, 2022.

[12] B. A. Garner, Ed., *Warranty, BLACK'S LAW DICTIONARY (12th ed.)*, 2024.

[13] *Uniform Commercial Code (UCC) §2-313*. AM. LAW INST. & Unif. Law Comm'n, 2023.

[14] *Uniform Commercial Code (UCC) §2-315*. AM. LAW INST. & Unif. Law Comm'n, 2023.

[15] *Implied Warranty: Merchantability; Usage of Trade., Unif. Commercial Code §2-314*. AM. LAW INST. & Unif. Law Comm'n, 2023.

[16] B. A. Garner, Ed., *Disclaimer, BLACK'S LAW DICTIONARY (12th ed.)*, 2024.

[17] *Liability, BLACK'S LAW DICTIONARY (12th ed.)*, 2024.

[18] *RESTATEMENT (FIRST) OF CONTRACTS §326*. AM. LAW INST., 1932.

[19] D. B. DOBBS, P. T. HAYDEN, and E. M. BUBLICK, *THE LAW OF TORTS §1 (2nd ed.)*, 2024.

[20] *RESTATEMENT (SECOND) OF TORTS §282*. AM LAW INST., 1965.

[21] D. B. DOBBS, P. T. HAYDEN, and E. M. BUBLICK, *THE LAW OF TORTS §437 (2nd ed.)*, 2024.

[22] *RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. §1*. AM. LAW INST., 1998.

[23] *RESTATEMENT (SECOND) OF TORTS §901 cmt. a*. AM. LAW INST., 1965.

[24] *Uniform Commercial Code (UCC) §2-316*. AM. LAW INST. & Unif. Law Comm'n, 2023.

[25] *Bouvier Law Dictionary Exculpatory Clause, THE WOLTERS KLUWER BOUVIER LAW DICTIONARY DESK EDITION*, 2012.

[26] *Tunkl v. Regents of U. of Cal., 383 P.2d 441 (Cal. 1963)*, 1963.

[27] *RESTATEMENT (SECOND) OF TORTS §402A*. AM LAW INST., 1965.

[28] F. T. Commission, "About the FTC," https://www.ftc.gov/about-ftc, Accessed on Nov 10, 2024.

[29] *Federal Trade Commission Act, 15 U.S.C. §§41-58*.

[30] F. T. Commission, "Privacy and Security Enforcement," https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement, Accessed on Nov 10, 2024.

[31] F. C. Commission, "U.S. Cyber Trust Mark," https://www.fcc.gov/CyberTrustMark, Accessed on Nov 10, 2024.

[32] "89 C.F.R. 61242," 2024.

[33] S. Manandhar, K. Kafle, B. Andow, K. Singh, and A. Nadkarni, ""Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage," in *Proceedings of the 31st USENIX Security Symposium (USENIX)*, Boston, MA, USA, Aug. 2022, acceptance rate: 256/1414, 18

[34] V. Braun and V. Clarke, *Thematic Analysis: A Practical Guide*. SAGE Publications, 2021. [Online]. Available: https://books.google.com/books?id=eMArEAAAQBAJ

[35] B. A. Garner, Ed., *Damages, BLACK'S LAW DICTIONARY (11th ed.)*, 2019.

[36] *Lost Profits, BLACK'S LAW DICTIONARY (11th ed.)*, 2019.

[37] "Certification Mark – U.S. Cybersecurity Labeling Program for Smart Devices," https://www.fcc.gov/cybersecurity-certification-mark, last accessed on June 2024.

[38] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice," *Proceedings of the ACM on human-computer interaction*, vol. 3, no. CSCW, pp. 1–23, 2019.

[39] S. Klivan, S. Höltervennhoff, R. Panskus, K. Marky, and S. Fahl, "Everyone for Themselves? A Qualitative Study about Individual Security Setups of Open Source Software Contributors," in *2024 IEEE Symposium on Security and Privacy (SP)*, 2024, pp. 1065–1082.

[40] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into iot device purchase behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1–12. [Online]. Available: https://doi.org/10.1145/3290605.3300764

[41] "National Institute of Standards and Technology," https://www.nist.gov/, Accessed on Nov 10, 2024.

[42] J. Lerner and J. Tirole, "A model of forum shopping," *American economic review*, vol. 96, no. 4, pp. 1091–1113, 2006.

[43] A. Larsen, "Becoming a Doctrine," *Florida Law Review*, vol. 76, no. 1-57, 2024.

[44] P. Emami-Naeini, Y. Agarwal, L. Faith Cranor, and H. Hibshi, "Ask the Experts: What Should Be on an IoT Privacy and Security Label?" in *2020 IEEE Symposium on Security and Privacy (SP)*, May 2020, pp. 447–464.

[45] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2013, pp. 3393–3402.

[46] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, and L. F. Cranor, "Are Consumers Willing to Pay for Security and Privacy of IoT Devices?" pp. 1505–1522, Aug. 2023. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/emami-naeini

[47] R. Stevens, J. Dykstra, W. K. Everette, J. Chapman, G. Bladow, A. Farmer, K. Halliday, and M. L. Mazurek, "Compliance Cautions: Investigating Security Issues Associated with US Digital-Security Standards." in *In the Proceedings of the Network and Distributed Systems Symposium (NDSS)*, 2020.

[48] C. Cakebread, "You're not alone, no one reads terms of service agreements," *Business Insider*, vol. 15, no. 11, 2017.

[49] M. Sandelowski, "Real qualitative researchers do not count: The use of numbers in qualitative research," *Research in nursing & health*, vol. 24, no. 3, pp. 230–240, 2001.

[50] V. Braun and V. Clarke, "To saturate or not to saturate? questioning data saturation as a useful concept for thematic analysis and sample-size rationales," *Qualitative research in sport, exercise and health*, vol. 13, no. 2, pp. 201–216, 2021.

[51] R. E. Thompson, M. McLaughlin, C. Powers, and D. Votipka, ""There are rabbit holes I want to go down that I'm not allowed to go down": An Investigation of Security Expert Threat Modeling Practices for Medical Devices," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 4909–4926. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/thompson

[52] W. Zhou, Y. Jia, Y. Yao, L. Zhu, L. Guan, Y. Mao, P. Liu, and Y. Zhang, "Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 1133–1150. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/zhou

[53] Y. Nan, X. Wang, L. Xing, X. Liao, R. Wu, J. Wu, Y. Zhang, and X. Wang, "Are you spying on me? Large-scale Analysis on IoT Data Exposure through Companion Apps," in *Proceedings of the 32nd USENIX Conference on Security Symposium*, ser. SEC '23. USA: USENIX Association, 2023.

[54] D. Kumar, K. Shen, B. Case, D. Garg, G. Alperovich, D. Kuznetsov, R. Gupta, and Z. Durumeric, "All things considered: An analysis of IoT devices on home networks," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 1169–1185. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/kumar-deepak

[55] K. Kafle, K. Moran, S. Manandhar, A. Nadkarni, and D. Poshyvanyk, "Security in Centralized Data Store-based Home Automation Platforms: A Systematic Analysis of Nest and Hue," *ACM Transactions on Cyber-Physical Systems (TCPS)*, vol. 5, no. 1, Dec. 2020.

[56] X. Wang, Y. Sun, S. Nanda, and X. Wang, "Looking from the mirror: Evaluating iot device security through mobile companion apps," in *Proceedings of the 28th USENIX Security Symposium (USENIX)*, 2019, pp. 1151–1167.

[57] E. Chatzoglou, G. Kambourakis, and C. Smiliotopoulos, "Let the Cat out of the Bag: Popular Android IoT Apps under Security Scrutiny," *Sensors*, vol. 22, no. 2, p. 513, 2022.

[58] D. M. Junior, L. Melo, H. Lu, M. d'Amorim, and A. Prakash, "A study of vulnerability analysis of popular smart devices through their companion apps," in *2019 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2019, pp. 181–186.

[59] K. Kafle, K. Moran, S. Manandhar, A. Nadkarni, and D. Poshyvanyk, "A Study of Data Store-based Home Automation," in *Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY)*, Mar. 2019.

[60] B. Chen, T. Wu, Y. Zhang, M. B. Chhetri, and G. Bai, "Investigating users' understanding of privacy policies of virtual personal assistant applications," in *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*, 2023, pp. 65–79.

[61] "Cybersecurity Labelling Scheme (CLS)," https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme.

[62] "Evidencing the cost of the UK government's proposed regulatory interventions for consumer IoT," https://assets.publishing.service.gov.uk/media/5f0da46ed3bf7f03aa74a79d/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products_-_technical_report.pdf.

[63] T. W. House, "The President's Executive Order (EO) 14028 on Improving the Nation's Cybersecurity," https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, May 2021.

[64] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, and L. F. Cranor, "An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices," *IEEE Security & Privacy*, vol. 20, no. 2, pp. 31–39, Mar. 2022.

[65] T. Li, K. Reiman, Y. Agarwal, L. F. Cranor, and J. I. Hong, "Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels," in *CHI Conference on Human Factors in Computing Systems*. New Orleans LA USA: ACM, Apr. 2022, pp. 1–24.

[66] J. Haney, Y. Acar, and S. Furman, ""It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security," in *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 411–428. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/haney

[67] L. Kustosch, C. Gañán, M. van 't Schip, M. van Eeten, and S. Parkin, "Measuring up to (reasonable) consumer expectations: Providing an empirical basis for holding IoT manufacturers legally responsible," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 1487–1504. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/kustosch

[68] S. D. Johnson, J. M. Blythe, M. Manning, and G. T. W. Wong, "The impact of IoT security labelling on consumer product choice and willingness to pay," *PLOS ONE*, vol. 15, no. 1, p. e0227800, Jan. 2020.

[69] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, and L. F. Cranor, "Which privacy and security attributes most impact consumers' risk perception and willingness to purchase iot devices?" in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 519–536.

TABLE 3: The details of IoT vendors.

ID	Vendor Name	Vendor Website	Terms and Conditions Link on Website
V1	Wyze	https://www.wyze.com/	https://www.wyze.com/policies/terms-of-service
V2	Tuya	https://www.tuya.com/	https://auth.tuya.com/policies/service
V3	Roku	https://www.roku.com/	https://docs.roku.com/published/tos/en/us
V4	Midea	https://www.midea.com/us	https://www.midea.com/us/terms-of-use
V5	Ring	https://ring.com/	https://ring.com/terms
V6	Afero	https://www.afero.io/	https://www.afero.io/html/home/privacy.html#general
V7	iRobot	https://www.irobot.com/	https://iot-content.irobot.com/eula
V8	Blink	https://blinkforhome.com/	https://blinkforhome.com/terms-of-service
V9	Yi Home	https://yitechnology.com/	https://yitechnology.com/legal/terms-of-use
V10	GoSund	https://us.gosund.com/	https://us.gosund.com/pages/terms-of-service
V11	Vicohome	https://vicohome.io/	https://vicohome.io/terms_of_service?
V12	Nuki	https://nuki.io/en/	https://nuki.io/en/service/terms-and-conditions/
V13	Wink	https://www.wink.com/	https://www.wink.com/legal/#tos
V14	Samsung	https://www.samsung.com/us/	https://www.samsung.com/us/common/legal/
V15	Remootio	https://remootio.com	https://www.remootio.com/policies/terms-of-service
V16	ilifesmart	https://iot.ilifesmart.com/	https://iot.ilifesmart.com/terms-of-use/
V17	1home	https://www.1home.io/	https://www.1home.io/legal/terms-and-conditions
V18	Angelcam	https://www.angelcam.com/	https://www.angelcam.com/terms
V19	alarm.com	https://www.alarm.com/	https://www.alarm.com/terms_conditions.aspx
V20	Alfred	https://alfred.camera/	https://alfred.camera/terms-and-conditions

[70] D. G. Balash, M. M. Ali, C. Kanich, and A. J. Aviv, ""i would not install an app with this label": Privacy label impact on risk perception and willingness to install iOS apps," in *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 413–432. [Online]. Available: https://www.usenix.org/conference/soups2024/presentation/balash

[71] S. Vetrivel, V. van Harten, C. H. Ganan, M. van Eeten, and S. Parkin, "Examining consumer reviews to understand security and privacy issues in the market of smart home devices," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 1523–1540. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/vetrivel

Appendix A. Vendor Information

Appendix B. Document Analysis Codebook

TABLE 4: The codebook developed during our document analysis in collaboration with security and law researchers.

Code	Explanation	Example
At your own risk At your sole risk At their own risk	Phrases when discussing assumed risk	*Your use of our Products and Services is at your sole risk.*
Permitted by law Applicable law Jurisdiction	Phrases when discussing exceptions under applicable law	*...herby disclaim, to the fullest extent permitted by applicable law, all warranties ...*
In no event Under no circumstances	Phrases leading into limitations	*Under no circumstances will <vendor> be responsible or liable to you for ....*
Affiliates Employees Contractors Agents Trustees	Terms used when listing affiliates who will also not be liable	*In no event will we, or any of our respective ... affiliates ... be liable to you or anyone else for ...*
Form of action Cause of action Legal theory	Phrases leading into the types of action that will not be permitted	*...regardless of the form of action...*
Damage(s)	Term used when discussing the various types of damages that will not be permitted	*... we will not be responsible for any indirect, special, consequential, exemplary, or punitive damages*
Shall not exceed Limited to Aggregate Cumulative	Phrases used when discussing limitations on allowable damages	*The total liability... is limited to the greater of ...*
Limited warranty Express or implied	Phrases used when discussing warranties	*... does not make any warranty of any kind, whether express or implied, including but not limited to ...*

Appendix C.
Survey Instruments

Survey Questions

. . . . . .

Consent Form *(We provide our informed consent form here)*

Section 0: Definitions of terms used in this survey
This section describes the definitions of terms used in this survey in the order of appearance. You can download a copy of these definitions from this link if you need them later to complete the survey.

IoT Device: A device designed to perform a specific function with the support of network connectivity. IoT Devices use built-in sensors and software to gather data and connect the physical world to digital systems. Most IoT Devices are connected to the Internet to send information (e.g., device status) or receive remote commands from the device owner (e.g., a house thermostat changes temperature based on its user adjusting the device setting on a mobile app).
IoT Companion/Controller App: A companion or controller application that allows users to interact remotely with their IoT Device. For instance, users of Ring cameras can watch over their property remotely and get instant motion or activity alerts through the Ring companion app.
IoT Vendor: A business that manufactures and/or sells IoT Devices.
Standards Body: An organization or a group of organizations that develop IoT security standards establishing baseline security criteria for IoT Devices (e.g., Google Nest) and their Companion/Controller Apps (e.g., Google Home). For example, the ioXt Alliance has developed the ioXt standard to certify IoT Devices.
Certification Standards: The IoT security standards developed by Standards Bodies to set the baseline security criteria for IoT Devices and their Companion/Controller App.
Certification Labs: Organizations that perform security assessments and provide certifications based on the Certification Standards developed by Standards Bodies. Some examples of Certification Labs include Capgemini, DEKRA, and Red Alert Labs.
Compliance Certificate: A document issued by Certification Labs indicating IoT Devices' compliance with the relevant Certification Standards developed by the Standards Body. An example of a Compliance Certificate is the ioXt SmartCert Program.
Vulnerabilities: Known security defects that security assessments and assessors ought to have discovered. Vulnerabilities are documented problems within the scope of the IoT Security standards developed by Standards Bodies. For the purpose of this survey, they exclude zero-day vulnerabilities or security defects not known to the wide security community.

Section A: Background Information
This section asks about some background information about you. As stated in the consent form, all such details will be anonymized before publication, and no information about you or the organizations will be disclosed.
1 *What is your current job status?* ○ Employed full time ○ Employed part time ○ Retired ○ Prefer not to say ○ Other (Please specify) _____
2 *How many years of professional experience do you have as a law practitioner? (in years)* _____
3 *Please state the field you are working as a legal practitioner.* _____

Section B: Familiarity with IoT Companion/Controller Apps, IoT Vendors, Standards Bodies, and Certification Labs
This section asks questions about your familiarity with IoT Companion/Controller Apps, IoT Vendors, Standards Bodies, and Certification Labs.
If you have working experience with any of them as a legal practitioner, provide as many details as possible about your involvement. As stated in the consent form, all such details will be anonymized before publication, and no information about you or the organizations/vendors indicated in this response will be disclosed.
4 *How familiar are you with IoT Devices? For the scope of this survey, being familiar could mean that you know about IoT devices, whether or not you use them (or have used them in the past).* ○ Extremely familiar ○ Very familiar ○ Moderately familiar ○ Slightly familiar ○ Not familiar at all
5 *How familiar are you with IoT Companion/Controller Apps? For the scope of this survey, being familiar could mean that you know about IoT companion apps (e.g., Google Home, Samsung SmartThings), whether or not you use them (or have used them in the past).* ○ Extremely familiar ○ Very familiar ○ Moderately familiar ○ Slightly familiar ○ Not familiar at all
6 *Do you have any experience working with any IoT Vendors? If "yes", provide as many details as possible about your involvement.*

○ Yes. _____ ○ No

7 *Do you have any experience working with any Standards Bodies? If "yes", provide as many details as possible about your involvement.* ○ Yes. _____ ○ No

8 *Do you have any experience working with any Certification Labs? If "yes", provide as many details as possible about your involvement.* ○ Yes. _____ ○ No

Section C: Perceptions regarding Liability in the event of security failures in IoT

We will now ask you about your opinion regarding liability in the event of a cyber incident caused by a Vulnerability present in an IoT Device that had received a Compliance Certificate from a Certification Lab.

We want to explore with you, in the event of a cyber incident, who you think is liable, who should be liable, and whether you are aware of any practices (for instance, limitation or exclusion of liability clauses in contracts) that limit or eliminate liability.

The questions will explicitly state if you can select multiple choices as answers.

Scenario 1: *An IoT Device (e.g., a baby monitor, smart air conditioner, or smart camera) that received a Compliance Certificate issued by a Certification Lab has a Vulnerability that allows an attacker to steal sensitive audio/video data that is sent by the device to the IoT Companion/Controller App.*

Scenario 2: *Consider this variation to scenario 1: An IoT Device that received a Compliance Certificate issued by a Certification Labs has a vulnerability outside of the scope of the Certification Standards.*

Participants were asked Q9→Q17 for both of these scenarios.

9 *How would you rate the severity of this scenario? Please select one of the options, which are organized from the highest (critical) to lowest (not severe) severity levels.* ○ Critical severity ○ High severity ○ Medium severity ○ Low severity ○ Not severe at all

10 *Do you think who is responsible for ensuring the security compliance of the IoT Device? (Please select all that apply.)* □ IoT Vendor □ Certification Lab □ Standards Body □ User □ No one □ Don't know □ Other._____

11 *Please explain your response to the previous question.*

_____

12 *If the exploitation of the Vulnerability causes the user of the IoT Device a legally-actionable harm, who should be liable for it?(Please select all that apply.) Please remember that we define Vulnerabilities as known security defects that security assessments and assessors ought to have discovered using the Standards Body's Certification Standards.* □ IoT Vendor □ Certification Lab □ Standards Body □ User □ No one □ Don't know □ Other._____

13 *Please explain your response to the previous question.*

_____

14 *If the exploitation of the Vulnerability causes the user of the IoT Device a legally-actionable harm, who is liable for it? (Please select all that apply.) Please remember that under our definition, Vulnerabilities are known security defects that security assessments and assessors ought to have discovered using the Standards Body's Certification Standards.* □ IoT Vendor □ Certification Lab □ Standards Body □ User □ No one □ Don't know □ Other._____

15 *Please explain your response to the previous question.*

_____

16 *Bearing in mind our definition of Vulnerability, does your view on who should be liable change if it is established that the contract between the IoT Vendor and the Certification Lab contains a clause that (i) limits the Certification Lab's liability to the IoT Vendor to a low sum of money, and (ii) excludes any consequential damages to the IoT Vendor and third parties, such as users.* ○ Yes. _____ ○ No

17 *Please explain your response to the previous question.*

_____

Section D: Regulatory Landscape

This section asks questions about your familiarity with regulatory landscape for IoT.

18 *In March 2024, the Federal Communications Commission adopted rules for its IoT Cybersecurity Labeling Program, the "U.S. Cyber Trust Mark.". Are you aware of this program?* ○ Yes ○ No

19 *If you are aware of this program, please share up to three positive features of this program, or potential positive impact it may have in your opinion.* _____

20 *If you are aware of this program, please share up to three negative features of this program, or potential positive impact it may have in your opinion.* _____

21 *How likely do you think is that this program will be used by IoT Vendors?* ○ Extremely likely ○ Somewhat likely ○ Neither likely nor unlikely ○ Somewhat unlikely ○ Extremely unlikely

22 *How likely do you think is that this program will be recognized by consumers?* ○ Extremely likely ○ Somewhat likely ○ Neither likely nor unlikely ○ Somewhat unlikely ○ Extremely unlikely

23 *What do you think will determine the success of the program?*

_____

24 *Thinking about the Federal Trade Commission's enforcement actions pertaining to consumer IoT Devices (e.g., Ring doorbell and wireless camera devices), do you think that the risk of enforcement actions has an impact on how IoT Vendors approach security compliance?* ○ Yes ○ No

25 *Please explain your response to the previous question.*

_____

Section E: Demographic Information

This section asks about demographic information (particularly age, gender, and education). All questions are optional.

26 *How do you identify yourself in terms of gender?* ○ Male ○ Female ○ Non-binary / third gender ○ Prefer not to say ○ Other _____

27 *What is your age?* ○ 18-29 years old ○ 30-39 years old ○ 40-49 years old ○ 50-64 years old ○ 65 years or older ○ Prefer not to say

28 *What is your highest level of education?* ○ Some college ○ Vocational degree ○ Bachelor's degree ○ Professional degree ○ Master's degree ○ Doctorate ○ Prefer not to say

Additional Question

29 *Is there any additional information you would like to provide to help us understand your responses or improve the survey? (Optional)* _____

End of our survey

. . . . . .

Appendix A.
Meta-Review

The following meta-review was prepared by the program committee for the 2025 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

A.1. Summary

This paper explores liability for vulnerabilities in certified IoT products through analysis of 20 end-user license agreements and terms of service and a survey with 18 legal professionals. The analysis identified 14 key findings, such as drafting clauses to minimize liability as much as possible (sometime illegally) and that IoT vendors' security expectations and legal professionals' security expectations differ. The results are used to build a legal framework for guiding various stakeholders in what to expect when there is harm resulting from security vulnerabilities.

A.2. Scientific Contributions

- Provides a Valuable Step Forward in an Established Field
- Addresses a Long-Known Issue
- Independent Confirmation of Important Results with Limited Prior Research

A.3. Reasons for Acceptance

1) This paper is very well-written and easy to read.
2) This paper explores an understudied and important topic of IoT legal liability through both an analysis of documents and interviews with legal experts.
3) The results are interesting and impactful and offer strong and actionable recommendations for both vendors and legal experts.