Table 1: Participant Demographic Information

		Participants n=76	
		n	%
Gender	Male	51	67.11
	Female	24	31.58
	Prefer not to say	1	1.32
Age	18-29 years old	37	48.68
	30-39 years old	33	43.42
	40-49 years old	5	6.58
	50-64 years or older	1	1.32
Education	Less than high school	1	1.32
	High school or equivalent	4	5.26
	Some college	22	28.95
	Bachelor's degree	29	38.16
	Doctorate	5	6.58
	Masters	12	15.79
Job Status	Employed at an organization	38	50
	Freelancer	17	22.37
	Both (i.e., work as a freelancer in my free time in addition to being full-time employed)	21	27.63

1 Survey Results

This section describes the results from our analysis of 76 survey responses. We leveraged these initial results to prioritize questions in our interview guide.

Table 1 provides demographic information about our participants. Among 76 survey participants, 51 (67.11%) were male and 24 (31.38%) were female. Most of our participants were between 18 and 40 years old. More than 50% participants were employed in an organization. Our survey participants have an average of 5 years of industry experience, with a maximum 15 years of experience.

The majority of participants (70/76 or 92.11%) agree that IoT security standards are important for the security of the product because *products with compliant safety standards are generally more trusted by consumers*. Most participants (67/76 or 88.15%) believe that compliance certification positively impacts IoT product security. The rest participants think that the certification has no impact, i.e., the product would be just as secure (or vulnerable) without it.

Most participants hold developer (67/76 or 88.16%) and certification labs (63/76 or 82.89%) liable if a vulnerability within the scope of the certification standard is found in the certified product, as one of the participants states,*"Everyone is responsible if there is a bug in the product"*. Further, as shown in Figure 1, we observe similar sentiment when participants were asked about who is liable, based on a hypothetical scenario about the information leak from a certified IoT app. While a majority (58/76 or 76.32%) participants agree that a vulnerability in a certified product indicates a failure of the security compliance process, only 10/76 (13.15%) participants believe that *a vulnerability in a certified product doesn't necessarily mean the whole security compliance process is a failure.*

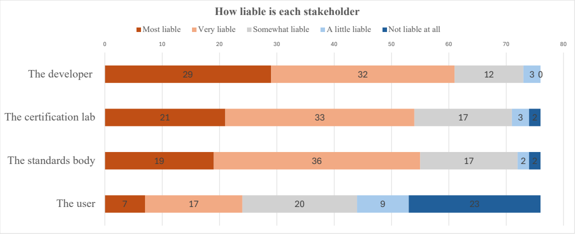

Figure 1: How liable is each stakeholder?