Supplementary Material for the Paper Where Are the Red Lines? Towards Ethical Server-Side Scans in Security and Privacy Research

1. Interview Guides

1.1 Members of Research Ethics Committees

TABLE 5. INTERVIEW GUIDE FOR ETHICS COMMITTEE MEMBERS

Part	Questions and Explanations
	Do you consent to participating in this interview, its recording of it, and it being transcribed via Amberscript?
REC	What are currently the main ethical challenges for cyber-security research? What were most difficult cases you had to decide while acting in your capacity as REC member? How many members are there in the ethics committees of the main conferences? How do you recruit members for ethics committees? Do committees remain quite stable in terms of personnel over longer periods of time or is there a lot of fluctuation?
Ethics in Research	Have you ever assessed security studies (planned projects or submitted papers) that used 3S techniques? What were key ethical issues in these studies? From the ethical point of view, how do you assess 3S as a method of data-gathering in security studies? Are there any controversial 3S topics among the members of the committee? How far can security researchers go when testing the behavior of internet infrastructure and websites? Can there be *gray areas* when it comes to studies using 3S techniques and testing of Internet infrastructure? If so, what are these *gray areas*? How should researchers who operate in such *grey areas* be assessed from an ethical perspective? Can you identify absolute *red lines* when it comes to the use of 3S techniques for security research purposes? If so, what are these *red lines*? How would you justify each of these *red lines*? How do you see the relationship between ethical norms regulating scientific research and legal norms? Should security researchers be allowed to do everything that is legal? If not, how would you justify ethical restrictions that go beyond legal restrictions? Should security researchers be allowed to act illegally if it benefits science and/or the broader society? If yes, what would justify such transgressions of legal norms? What should be the absolute normative boundary for such law-transgressive security research? Who should be authorized to decide if a legal transgression by a scientific research team is still acceptable? What kind of institutional safeguards are already in place or should be additionally created?
Improvements	Do you have specific ideas how the use of 3S techniques by security researchers should be regulated to maximize the benefit for all stakeholders (potentially) involved? What would you propose as key stipulations, if asked to design an ethical framework for 3S research? What would you add to the existing ethical framework regulating security research to make 3S studies beneficial? *Explaining our pre-registration proposal...* What do you think about it? How would you re-organize existing institutions tasked with control over security researchers' adherence to norms of scientific ethics? Are there serious flaws in currently existing institutions tasked with control over security researchers' ethics?
Outro	Is there something else you would like to share with us on the topic of ethical regulation of security research — in general or with regard to the use of 3S techniques?

1.2 Legal Experts

TABLE 6. INTERVIEW GUIDE FOR LEGAL EXPERTS. SOME QUESTIONS WERE ONLY FOR ACADEMICS (A), PROSECUTORS (P), OR LAWYERS (L).

Part	Questions and Explanations
	Do you consent to participating in this interview, its recording, and it being transcribed via Amberscript?
Intro	Where do you currently see as the most important or biggest challenges in the legal regulation of web security ? (A) What is currently being discussed in this field of legal research? (P) Which security phenomena relevant to criminal law are currently most present in your work as a prosecutor? Are attempts to exploit vulnerabilities of websites currently an important issue in legal debates in your domain? If yes, what exactly is being discussed? Where do you obtain the technical expertise when dealing with questions of legal regulation of digital topics? Are you familiar with the term *server-side scanning*? If yes, how would you define this term?
Criminal Law	What legal risks do you see in server-side scans that are carried out by researchers?
	What criminal consequences could arise for someone conducting such scans? Have there been cases where criminal prosecution has occurred due to such scientifically motivated tests? (P) (L) Were you involved in any of such cases? What were the results of these proceedings? What forensic means are used in such cases? What defense strategies are chosen by lawyers for those affected by the prosecution? How successful do you estimate these strategies to be? How does prosecution in such cases practically come about? (P) How can a prosecutor get information about an attack on a server? (P) Do authorities focus on filed reports or are there also active investigative against web attacks? (P) What other agencies besides your prosecutor's office are involved in prosecuting such cases? Which authorities are responsible for prosecution in such cases? Is there a corresponding specialization in the public prosecutor's offices? Is there a corresponding specialization in police stations or within state or federal police authorities? Who investigates in cross-border cases? Are there lawyers who specialize in such cases or became known for defenses in such cases?
Civil Law	What civil law consequences could arise for someone conducting such tests? Is this relevant for your work as a lawyer (L) / prosecutor (P)? (A) Have there been specific cases where civil lawsuits have been filed against someone conducting such tests? (A) How did these lawsuits come about? (A) What were the results of these proceedings? (A) What forensic means are used in such cases? (A) What strategies were chosen by the lawyers of the defendants? (A) Are there law firms that specialize in such lawsuits?
Legal Misc	Is privacy law relevant for someone conducting such tests? Are there other areas of law relevant for someone conducting such tests? Are there gray areas when conducting such tests? In relation to IT security, are there cases where the benefits for the general public outweigh a potential crime? Looking at the USA, we see they adjusted their *Computer Fraud and Abuse Act*. The attacker's intention is now also considered. The German coalition agreement mentions something similar. Do we currently see a shift in legislation? What is the current status here? How can such legal changes affect legal practice?
International	How does the law deal with cases of cross-border attacks on websites? How important is international law in cases of cross-border attacks on websites? What differences in legal protection of websites are there between different countries? What importance does European law have in this area? What importance does US law have in this area? The USA is not only the cradle of Internet technology, but to this day also the most important place for technological innovation. How does this fact affect the legal regulation of activities on the Internet? How does the fact that many components of the entire Internet infrastructure are not located in Germany or the EU affect the possibilities for legal regulation of activities (especially research activities) on the Internet? Are there different legal approaches in different countries when it comes to cases of web attacks?
Improvements	Do you see a way for researchers to legally conduct 3S? If someone asked you, how would you create a possibility to enable 3S for researchers? *Explain our pre-registration proposal...* What do you think about it?
Outro	In the case of publishing vulnerability analyses, what should researchers pay attention to? Is there something else you would like to share with us on the topic of 3S?

1.3 Operators

TABLE 7. INTERVIEW GUIDE FOR WEB OPERATORS

Part	Questions and Explanations
	Do you consent to participating in this interview, its recording, and it being transcribed via Amberscript?
Background	Please describe in what way you are responsible for a website. What is your daily (primary) job? How is the website maintenance related to your primary job (if related at all)? How did you build the website(s)? How do you maintain the website on a daily (ongoing) basis? How come that you know how to operate a website? Can you tell us a bit about your background? Did you learn programming at school / university? What kind of courses did you attend? Did you learn programming in specialized trainings / courses? What kind of specialized trainings did you attend? Did you teach programming yourself? How did you do that more specifically? What kind of knowledge sources were you using in this process?
IT Security	What are currently the main challenges for operators like you when it comes to hacking? Is the topic of hacking discussed among operators like you and your colleagues? How would you assess your security awareness as an operator? Where do you get the IT security knowledge from? Where do other operators get their IT security knowledge from? What role do interpersonal contacts with other operators play in your acquisition of new knowledge and skills? What is the role of online forums in acquiring IT-related knowledge? Were you ever involved in a vulnerability disclosing process? Can you go into more detail what happened there?
Server-Side Scanning	Are you familiar with the term *server-side scanning* (3S)? If so, how would you define it? Did you ever recognize someone conducting 3S on your server? If yes: Please tell me about your reaction / what you did after you noticed it. What is your general opinion about 3S? Should it be allowed for research purposes? Can you describe how you think 3S research is conducted? Should it be allowed for some other purpose? Do you see any problems for researchers doing 3S? Would you sue a researcher who conducted 3S on your IT infrastructure? Would the location of the IP address of the 3S actor make a difference? How far can security research go (in your opinion)? What are *gray areas*? Can you define absolute *red lines*? How would you justify these *red lines*? Do you see problems for you / your company resulting from 3S? What would happen if something breaks (after 3S)? What would happen if data is leaked (after 3S)? Would you analyze or look closer at traces of a 3S attempt? Would you improve your security after noticing 3S?
Improv.	Do you have any specific ideas how we could improve the current situation in a way that 3S is possible for researchers? If you were asked to design a guideline for security researchers, what would you propose? *Explain our pre-registration proposal...* What do you think about it?
Outro	Is there something else you would like to share with us on the topic of 3S?

2. Codebook

TABLE 8: INTERVIEW CODEBOOK

Level 1	Level 2	Level 3	Level 4	Uses
Actors	Institutions	Authorities		20
		BSI		55
		CERT		1
		Chaos Computer Club		5
		CISPA		13
		Ethics committee		25
		Intelligence agencies		1
		IRB		10
		ISP		1
		Researchers		17
		SOC		2
	Operators	Companies		30
		Operators in general		4
	Attorneys			11
	Business vs. research interest			3
	Cyber-criminals			2
	Hackers, malicious			10
	Hackers, white-hat			24
	James Kettle			2
	Organizational embeddedness			10
Additional Resources	Court rulings			30
	Encore paper [15]			3
	Experts			25
	Extant data, potential			1
	Hypocrite Commits paper [72]			8
	Legal commentaries			7
	Legal databases			2
	Menlo Report [8]			3
	Publications			46
	Sec4Research [9]			4
	Websites			8
Analogies	Car repair analogy			1
	Door and key analogy			10
	Driver's license analogy			1
	Financial market regulation analogy			1
	Journalist analogy			2
	Medical research analogy			6
	Narcotics analogy			3
	Nuclear power analogy			2
	Passive consent analogy			1
Assessments	Ethical	1 Unacceptable (ethics)		10
		2 Rather unacceptable (ethics)		10
		3 Ambiguous assessment (ethics)		8
		4 Towards acceptable (ethics)		12
		5 Acceptable (ethics)		13
		Unsure (ethics)		3
	Feelings	Bad feeling		9
		Mixed feelings		5
		Good feeling		1

Continued on next page

TABLE 8 – *continued from previous page*

Level 1	Level 2	Level 3	Level 4	Uses
Assessments	Legal	1 Illegal (law)		28
		2 Towards illegal (law)		40
		3 Legal gray zone (law)		13
		4 Towards legal (law)		34
		5 Legal (law)		21
		Unsure (law)		4
	Operators	1 Harmful (operator)		33
		2 Problematic (operator)		20
		3 Difficult (operator)		12
		4 Rather acceptable (operator)		10
		5 OK (not harmful; operator)		47
	Proposal	1 Bad idea		8
		2 Towards bad idea		1
		3 Idea developable		8
		4 Quite good idea		7
		5 Great idea		8
		No statement		1
	Professional opinions diverging			40
Case Study	Alice			27
	Bob			25
	Charlie			26
	Daisy			24
	Eve			25
	Additional case			29
	Case study boundaries			2
Improvements	Third-party approval ex-ante			36
	Approval research community			4
	BSI cooperation			14
	Exception for researchers			43
	Fixed IP address			4
	Low load			4
	Operator permission			28
	Our proposal			22
	Proposal feasibility			9
	Researcher definition			27
	Transparency			24
	General suggestions for improvement			58
	Work with partners			2
Information Sources	Academic embeddedness			9
	Blogs			1
	ChatGPT			5
	Conferences			6
	Google			3
	Hands-on			15
	Inter-personal contacts			9
	Internet forums			2
	Joint projects tech & law			5
	News			2
	No information sources			2
	Periodicals			5
	Tech knowledge sources			10
	Technical literature			9
	Training / Certificates			14
	University education			15
	Unspecified			2

Continued on next page

TABLE 8 – *continued from previous page*

Level 1	Level 2	Level 3	Level 4	Uses
Global	Asia			7
	Cyber Resilience Act			1
	Convention on Cybercrime			5
	Europe			22
	International legal differences			35
	Server location			17
	NIS2			3
	Oceania			1
	South America			1
	United States			39
Interview	Background			36
	Cannot disclose			4
	Case-Studies general-assessment			2
	Clarifying technicalities			62
	Cooperation offer			2
	Definition clarification			24
	Difference lawyers vs. academics			5
	Difference lawyers vs. technologists			2
Law	Criminal Law	Elements of offenses	Access protection	34
			Attempted vs. completed	2
			Data manipulation	28
			Consent	6
			Negligence	15
			Motivation	11
			Intention of causing damage	9
			Preparatory act	4
			Unlawfulness / justificatory defenses	14
			Guilt	3
			Intent	37
			Substantial importance	2
		Criminal law in general		79
		Sec. 202		25
		Sec. 202a		47
		Sec. 202b		10
		Sec. 202c		19
		Sec. 269		2
		Sec. 303		14
		Sec. 303a		37
		Sec. 303b		19
		Sec. 303c		0
		Sentencing		6
		Criminal procedure		37
		Forms of participation		2
	Civil Law	Terms of service		8
		Civil procedure		11
		Civil law in general		47
		Damages		46
		Injunctive relief		13
		Responsibility		11
	Privacy Law	Federal Data Protection Act (BDSG)		35
		Data protection legislation (other countries)		6
		GDPR		29
		Privacy law in general		49
		State data protection law		5

Continued on next page

TABLE 8 – *continued from previous page*

Level 1	Level 2	Level 3	Level 4	Uses
Law	Law enforcement practice	Law enforcement authority	General	13
			Police	21
			Prosecutor's office	37
		Courts		8
		Criminal complaint		29
		Decision to prosecute		12
		IT forensics		4
		Law enforcement practices in general		44
	Liability for breach of official duty			1
	Labor law			5
	Competition law			3
	Constitutional law			5
	Copyright law			15
	No double jeopardy			2
	Employee responsibility			11
	Freedom of the press			1
	IT law (general)			15
	Intellectual property law			1
	International law			16
	IT law (security)			11
	Legal reasoning			21
	Legal complexity			6
	Legal strategies			6
	Legal uncertainty			18
	Compulsory prosecution			8
	Regulatory offenses			5
	Press laws			2
	Privacy / confidentiality intended			4
	Criminal code			28
	Tax law			1
	Telecommunication law			2
	Administrative law			2
Normative Ideas	Ethical Frameworks	Accounting for power dynamics		1
		Changing ethical norms		2
		Deontology		12
		Different ethics approaches		12
		Discourse ethics		5
		Ethics modeling		2
		Normative colonialism		2
		Normative pluralism		7
		Ethical dilemma		5
		Utilitarianism		16
		Virtue ethics		1
	Ethics – Law	Ethics – Law		13
		Illegal but ethical		5
		Legal boundaries unclear		1
		Legal but unethical		5
	Harm and benefits	Avoiding damage / harm		40
		Generating appropriate benefits		11
		Harm vs. benefit		28
		No past harm		3
		Predicting benefits		2
		Predicting harm		22
		Quantifying harm		11

Continued on next page

TABLE 8 – *continued from previous page*

Level 1	Level 2	Level 3	Level 4	Uses
Norm. Ideas	Ethical review vs. IRB			3
	General problems (ethics)			7
	Human rights			1
	No fixed rules			16
	Public interest			27
Operator Problems	Alarm threshold			13
	Asset management			12
	Attack surface			3
	Bug bounty			10
	Community change-resistant			4
	Compliance			6
	Cost			20
	Security challenges (general)			6
	Fast technological change			4
	General problems (operators)			18
	Human factor in security			3
	Identify attacker			21
	IP blocking			18
	Lack of security awareness			7
	Lack of security knowledge			14
	Load high			23
	Load low			5
	Monitoring (operators)			9
	Notify authorities			16
	Notify customers			3
	Privacy incident			22
	Reputation			29
	Responsibility diffusion			4
	Security strategies			21
	Server crash			38
	Software security			2
	Staff availability			5
	Third-party components			8
	Tradeoff security–functionality			5
	Ubiquitous attacks			22
	User authentication			3
Politics	Coalition agreement			10
	Cyber-geopolitics			2
	Difference lawmakers vs. technologists			1
	Federalism			4
	Legislative policy			35
	Political landscape			9
	Stakeholder dialogue			1
	Technological progress $\rightarrow$ regulatory challenge			4
Practice	Real-world cases	Cases (3S)		14
		Cases (ethics)		20
		Cases (legal)		56
		Cases (operator)		44
	Attorney–client privilege			2
	Circumvention strategies			2
	Consulting legal			3
	Critical infrastructure			8
	Crypto currency			3
	Cyber insurance			2
	Hospital server			10
	Illegal research			2

Continued on next page

TABLE 8 – *continued from previous page*

Level 1	Level 2	Level 3	Level 4	Uses
Practice	Informing subjects			2
	Injunction			1
	Medical device vulnerability			2
	Pentesting			15
	Port scanning			10
	Ransomware			6
	Reverse engineering			5
	Risk aversion			6
	SQL injection			5
	Vulnerability disclosure			63
Review Process	Authors' reaction			1
	Authors' responsibility			2
	Conflicts			10
	Process explanation			14
	REC improvements			8
	REC shortcomings			6
Server-Side Scans	Assessments	Red lines		65
		Gray areas		22
		Accepted scans		49
	Normative Implications	Ability to consent		9
		Always unethical research		2
		Avoiding unintended consequences		27
		Considering alternative research designs		51
		Disclose incidents		16
		Documentation of experiment		2
		Following community best practices		6
		Informed consent		35
		No data leakage		38
		No data modification		12
		No own code execution		17
		Opt-out		2
		Own responsibility		28
		Papers' ethics discussion		6
		Scale of measurements		16
	3S (general assessment)			48
	3S experience (own)			26
	Changes after consent			2
	Data minimization			13
	Lawsuit			17
	Monitoring			3
	Points of contact			5
	Pre-testing study setup			20
	Problems due to 3S			24
	Problems executing 3S			20
	Reactions to harm done			11

3. Operator Survey Questionnaire

Welcome Page

Welcome!

We are security and privacy researchers from the CISPA Helmholtz Center for Information Security in Germany.

In our current research we aim to understand what types of server-side security scans Web operators are comfortable with. This will help define the boundaries of ethical Web security research and increase the chances that future security studies do not cause undue harm to Web operators' systems.

You can help us identify the "do's and don'ts" of server-side scans through completing this survey. The survey is anonymous, and all questions are optional, so please feel free to skip any questions you are uncomfortable with. Your feedback is very valuable to us and we really appreciate your time.

To learn more about us and this study, please visit our study website at https://server-side-study.cispa.de/.

Please click the arrow button below to proceed.

Privacy Policy & Consent

[Privacy policy for CISPA's Qualtrics instance, single-choice Yes / No question to obtain consent for data processing]

3.1 Background

First we would like to learn a bit about your background with web servers / websites.

Q1 Do you have experience with operating a web server / website? [single choice: Yes / No / Don't know]

Q2 **If Yes:** Please estimate how many web servers / websites you have operated **in the last 3 years**: [numeric input]

Q3 Which of the following roles most closely describes your **current main role** with regard to the operation of web servers / websites? [single choice]
- Security Engineer
- System Engineer
- Database Engineer
- Frontend Developer
- Backend Developer
- Full-stack Developer
- DevOps
- Management
- IT Consultant
- Penetration Tester
- Content Creator
- Other: [free text]

Q4 Please estimate the size of the largest organization (in number of people) for which you are currently operating web servers / websites? [Numeric input plus "Don't know"]

Q5 What is the location of the headquarters of the largest organization for which you are currently operating a web server / website? [dropdown list with list of independent countries]

3.2 Introduction to Server-Side Scans

Our survey investigates the ethics of server-side scans, so we first would like to define this term for the rest of the survey.

A **server-side scan** is an automated series of requests to systematically check a large number of web servers / websites for specific server-side behavior, such as potential vulnerabilities like SQL injections. The goal of such scans is to measure the prevalence of these issues. Thus, server-side scans can help identify common security loopholes, assess the robustness of security protocols, and, in turn, help to fortify server security.

Q6 How comfortable would you be with researchers conducting such server-side scans on your web servers / websites without prior notice? [single choice on Likert scale: Comfortable, Somewhat comfortable, Neither comfortable nor uncomfortable, Somewhat uncomfortable, Uncomfortable]

3.3 Intro Text for Scenarios

Now that we defined server-side scans, we will show you **five different scenarios** of how researchers could possibly interact with your web servers / websites.

Please read each scenario and indicate how comfortable you would be with the described actions being performed on your web servers / websites.

In all scenarios described in the following, assume that the researcher acts without prior notice but later discloses any found vulnerabilities to you as the operator.

The following scenarios A – E were shown in random order.

3.4 Alice

Imagine a researcher conducting the following scan on a large number of web servers / websites, including yours:

Researcher Alice checks web servers / websites for vulnerable database queries (e. g., via SQL injection). She uses a function to delay the database response by 1 second (e. g., the MySQL function "SLEEP"). This allows her to verify whether the web server / website is vulnerable or not.

A1 How comfortable would you be with Alice conducting such scans on your web server / website?
[single choice on Likert scale: Comfortable, Somewhat comfortable, Neither comfortable nor uncomfortable, Somewhat uncomfortable, Uncomfortable]

A2 **(If Comfortable, Somewhat comfortable, or Neither comfortable nor uncomfortable:)** How comfortable would you be with Alice using SQL injection to obtain the database structure?

[Comfortable ... Uncomfortable]

A3 **(If Neither comfortable nor uncomfortable, Somewhat uncomfortable, or Uncomfortable:)** How comfortable would you be with Alice using SQL injection to calculate 1+1 (e. g., SELECT 1+1) and verify that the payload returns 2?
[Comfortable ... Uncomfortable]

A4 Please explain your answers to the questions in the above scenario. [free text]

3.5 Bob

Imagine a researcher conducting the following scan on a large number of web servers / websites, including yours:

Researcher Bob sends a non-standard HTTP request to a web server / website. This causes the web server / website to crash **unintentionally** and it must now be restarted by its operator.

B1 How comfortable would you be with Bob conducting such scans on your web server / website?
[single choice on Likert scale: Comfortable, Somewhat comfortable, Neither comfortable nor uncomfortable, Somewhat uncomfortable, Uncomfortable]

B2 **(If Comfortable, Somewhat comfortable, or Neither comfortable nor uncomfortable:)** How comfortable would you be with Bob causing such an unintentional crash multiple times?
[Comfortable ... Uncomfortable]

B3 **(If Neither comfortable nor uncomfortable, Somewhat uncomfortable, or Uncomfortable:)** How comfortable would you be with Bob causing such an unintentional crash with an HTTP request that **conforms** with the standard?
[Comfortable ... Uncomfortable]

B4 Please explain your answers to the questions in the above scenario. [free text]

3.6 Charlie

Imagine a researcher conducting the following scan on a large number of web servers / websites, including yours:

Researcher Charlie changes his own user ID in the HTTP request to your web server / website to the ID of another user (e. g., `social-site.com/user/42` → `social-site.com/user/41`) and receives data from another user, e. g., their user name.

C1 How comfortable would you be with Charlie conducting such scans on your web server / website?
[single choice on Likert scale: Comfortable, Somewhat comfortable, Neither comfortable nor uncomfortable, Somewhat uncomfortable, Uncomfortable]

C2 **(If Comfortable, Somewhat comfortable, or Neither comfortable nor uncomfortable:)** How comfortable would you be with Charlie trying to **modify** the other user's data (e. g., the user name) with his scan?
[Comfortable ... Uncomfortable]

C3 **(If Neither comfortable nor uncomfortable, Somewhat uncomfortable, or Uncomfortable:)** How comfortable would you be with Charlie receiving data from another account that he also created himself?
[Comfortable ... Uncomfortable]

C4 Please explain your answers to the questions in the above scenario. [free text]

3.7 Daisy

Imagine a researcher conducting the following scan on a large number of web servers / websites, including yours:

Researcher Daisy exploits a stored XSS (Cross-Site Scripting) vulnerability to deliver the attack code to all users who access the vulnerable web page. The code is executed in these users' browsers and sends a confirmation message back to Daisy's server.

D1 How comfortable would you be with Daisy conducting such scans on your web server / website?
[single choice on Likert scale: Comfortable, Somewhat comfortable, Neither comfortable nor uncomfortable, Somewhat uncomfortable, Uncomfortable]

D2 **(If Comfortable, Somewhat comfortable, or Neither comfortable nor uncomfortable:)** How comfortable would you be with Daisy sending metadata about the user's browser (e. g., installed plugins) to her server instead of a confirmation message?
[Comfortable ... Uncomfortable]

D3 **(If Neither comfortable nor uncomfortable, Somewhat uncomfortable, or Uncomfortable:)** How comfortable would you be with Daisy still delivering the attack code to everyone but only sending the confirmation message from accounts she created herself?
[Comfortable ... Uncomfortable]

D4 Please explain your answers to the questions in the above scenario. [free text]

3.8 Eve

Imagine a researcher conducting the following scan on a large number of web servers / websites, including yours:

Researcher Eve accesses paths of your web server / website to read information that is supposed to be confidential but can be publicly viewed due to server misconfiguration (e. g., the configuration file of a Git repository).

E1 How comfortable would you be with Eve conducting such scans on your web server / website?
[single choice on Likert scale: Comfortable, Somewhat comfortable, Neither comfortable nor uncomfortable, Somewhat uncomfortable, Uncomfortable]

E2 **(If Comfortable, Somewhat comfortable, or Neither comfortable nor uncomfortable:)** How comfortable would you be with Eve accessing sensitive files that contain, e. g., user data or API keys?
[Comfortable ... Uncomfortable]

E3 **(If Neither comfortable nor uncomfortable, Somewhat uncomfortable, or Uncomfortable:)** How comfortable would you be with Eve accessing non-sensitive files such as `/etc/hosts`?

[Comfortable ... Uncomfortable]

E4 Please explain your answers to the questions in the above scenario. [free text]

3.9 Our Proposal

As you may have thought, great care must be taken in such server-side research to minimize potential harm. To improve this situation for all involved parties, we propose the concept of **prior approval of such scans** by a trusted third party, based on publicly known criteria.

A **trusted third party (TTP)** is an independent and transparent entity responsible for the assessment of server-side research proposals. The TTP evaluates the credibility of the research group and checks their proposed research methods to either approve or reject the proposal. In the future, only server-side research that has an approval from the TTP is considered ethical. This way, the TTP aims to minimize potential harm that could arise from such research.

Q7 Please indicate for the following institutions how competent you would consider them to act as the TTP who assesses server-side research proposals according to the above procedure:
[for each of the following, single choice on Likert scale: Competent, Somewhat competent, Neither competent nor incompetent, Somewhat incompetent, Incompetent]
- Government agency (e. g., BSI, FBI)
- Academic institution (e. g., universities)
- Industry institution (e. g., certification authority)
- Non-governmental organization / white-hat hacker organization (e. g., OWASP, CCC)
- International organization (e. g., EU, UN)

Q8 Assuming that such a trusted third party exists, how comfortable would you be with server-side scans approved by this trusted third party following the above procedure?
[single choice on Likert scale: Comfortable, Somewhat comfortable, Neither comfortable nor uncomfortable, Somewhat uncomfortable, Uncomfortable]

Q9 Which factors would be important to you to trust the approval procedure described above? [free text]

Q10 Knowing that a researcher obtained approval followed the above procedure, does this change your opinion on the previously described five scenarios (Alice, Bob, Charlie, Daisy, and Eve)?
[single choice: Yes, No, Don't know]

Q11a **(If Yes:)** In what way does this change your opinion? [free text]

Q11b **(If No:)** Why not? [free text]

3.10 Demographics

Finally, we would like to ask you some demographic questions to better understand who participated in our survey.

Q12 Have you ever received any kind of training or educated yourself on computer security? [single choice: Yes, No, Don't know]

Q13 **(If Yes:)** Please indicate which kind of prior security training or education you have received. [multiple choice]
- University / school
- Employer training
- Certifications
- Other courses outside of university, employer, or certifications
- "Learning by doing"
- Professional network
- Personal network
- Self-taught (e. g., via technical literature, online resources, ...)
- Other (please specify:) [free text]

Q14 What is your age in years? [numeric input]

Q15 What is your gender? [multiple choice; question by Spiel et al. [62]]
- Woman
- Man
- Non-binary
- Prefer not to disclose
- Prefer to self-describe: [free text]

Q16 Is there anything else you would like to tell us about this research or about server-side scans in general? [free text]

QEmail If you would like to be informed about the results of this study, please enter an email address for us to contact: [free text]

Appendix D. Meta-Review

The following meta-review was prepared by the program committee for the 2024 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers

D.1. Summary

This work takes a principled approach to constructing a normative framework for server-side scanning (3S) in the context of academic research, and legally under German law in particular. They perform a two-phase study: (1) interviews of legal scholars, research ethics committee members, and operators for qualitative understanding of ethical and legal concerns, and (2) a qualitative survey of system operators. The authors suggest that server-side scanning is generally well accepted by relevant parties and ultimately offer ethical guidelines to the community for future research.

D.2. Scientific Contributions

- Independent confirmation of important results with limited prior research
- Addresses a long known issue
- Provides a valuable step forward in an established field

D.3. Reasons for Acceptance

1) This paper independently confirms previously published ethical guidelines through a principled bottom-up approach based on stakeholder interviews/surveys.
2) This paper addresses the long known issue of server-side scanning, which has become increasingly common in the academic research community.
3) This work provides a valuable step forward in the ethics of security research by surfacing actionable results, some of which can generalize to other forms of Internet measurement.

D.4. Noteworthy Concerns

1) Insufficient upfront qualification/contextualization of results. The legal analysis is strictly limited to German law, which should be mentioned at the very beginning of the paper, and there is limited discussion of relevance to other legal jurisdictions. Additionally, the work does not reference key prior work to contextualize its findings.
2) Biased summarization of server-side testing acceptance. The study only highlights how many participants felt comfortable or somewhat comfortable, rather than how many don't. The summaries emphasize general acceptance of server side testing rather than pointing out that several (out of only 10) operators mentioned that they might be obligated to pursue legal remedies in the face of such vulnerability testing, in some cases regardless of the intention behind the testing.
3) Excessive generalization from few data points. The data in the paper is neither consistent nor sufficient (i.e., low number of participants) to draw sweeping conclusions, like that the operators have "a general positive stance" or "were generally open..." The participant selection process is also non-random so reported proportions can be misleading.
4) Shallow discussion of proposed trusted third-party (TTP) solution. The paper does not discuss the many obstacles to successfully implementing a TTP, thus misrepresenting its feasibility.