Open Universiteit

Ethics in CS research: a tale of two failures

Hugo Jonker

The cases

- Hypocrite commits (2021 S&P)
- CCPA Spam (2021, Princeton & Radboud)

Case #1: Hypocrite commits

The goal

- Check if Linux is resilient against “**hypocrite” commits**
  - Hypocrite commits: “seemingly beneficial minor commits that actually introduce other critical issues”

Execution

Testing the Linux kernel community

The trio's scheme involved first finding three easy-to-fix, low-priority bugs in the Linux kernel and then fixing them—but fixing them in such a way as to complete what the UMN researchers called an "immature vulnerability":

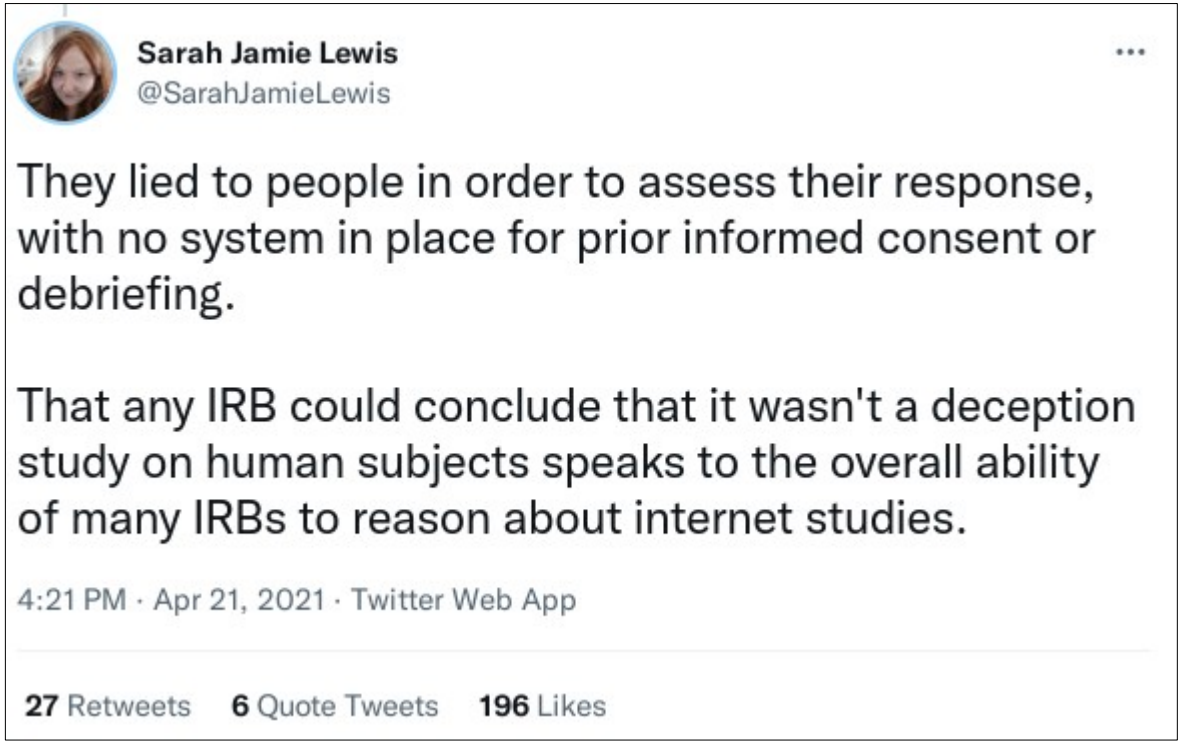
> We employ a static-analysis tool to identify three "immature vulnerabilities" in Linux, and correspondingly detect three real minor bugs that are supposed to be fixed. The "immature vulnerabilities" are not real vulnerabilities because one condition (such as a use of a freed object) is still missing [...] We construct three incorrect or incomplete minor patches to fix the three bugs. These minor patches however introduce the missing conditions of the "immature vulnerabilities."

The three researchers would then email their Trojan-horse patches to Linux kernel maintainers to see if the maintainers detected the more serious problem the researchers had introduced in the course of fixing a minor bug. Once the maintainers responded to the submitted patch, the UMN researchers pointed out the bug introduced by their patch and offered a "proper" patch—one that did not introduce a newly exploitable condition—in its place.

Lu, Wu, and Pakki published their findings in February at the 42nd IEEE Symposium on Security and Privacy.

The hullabaloo

The TL;DR



Sarah Jamie Lewis
@SarahJamieLewis

They lied to people in order to assess their response, with no system in place for prior informed consent or debriefing.

That any IRB could conclude that it wasn't a deception study on human subjects speaks to the overall ability of many IRBs to reason about internet studies.

4:21 PM · Apr 21, 2021 · Twitter Web App

27 Retweets **6** Quote Tweets **196** Likes

The follow-up

Initially:

- Vivid discussions in S&P program committee
- Discussions amongst Linux kernel devs
  - technical advisory board + volunteers investigate...
  - ... eradicate all Uni Michigan commits
  - ... find that they were not “hypocrite”

Eventually:

- Paper retracted by authors
- Uni Michigan banned from contributing to Linux kernel
- S&P implementing ethics, holds ethics panel

Case #2: CCPA Spam

The goal

- Understand how websites implement their obligations under privacy regulations (CCPA, GDPR) in practice

Execution

To Whom It May Concern:

My name is Maya Mishina, and I am a resident of Novosibirsk, Russia. I have a few questions about your process for responding to California Consumer Privacy Act (CCPA) data access requests:

1. Would you process a CCPA data access request from me even though I am not a resident of California?
2. Do you process CCPA data access requests via email, a website, or telephone? If via a website, what is the URL I should go to?
3. What personal information do I have to submit for you to verify and process a CCPA data access request?
4. What information do you provide in response to a CCPA data access request?

To be clear, I am not submitting a data access request at this time. My questions are about your process for when I do submit a request.

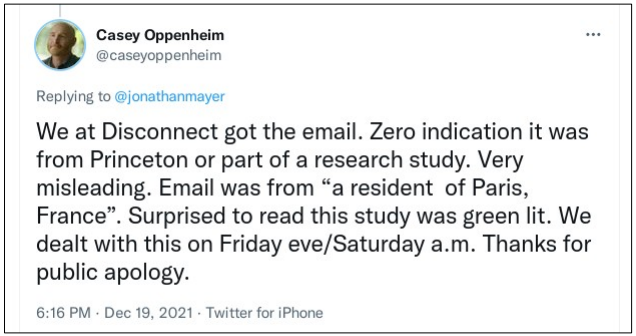
Thank you in advance for your answers to these questions. If there is a better contact for processing CCPA requests regarding christine.website, I kindly ask that you forward my request to them.

I look forward to your reply without undue delay and at most within 45 days of this email, as required by Section 1798.130 of the California Civil Code.

Sincerely,

Maya Mishina

Uproar on Twitter



The catch

I Was Part of a Human Subject Research Study Without My Consent

Update 2021-12-17: This is a human subject research study conducted Princeton University and Radboud University on unwitting persons. I verged on a panic attack for nothing. People who wasted money asking lawyers for their advice on this did it for nothing. How *dare* you, Princeton? I didn't give you permission to experiment on me!

The PI reacts

Note from Jonathan Mayer, the Principal Investigator

Hi, my name is Jonathan Mayer. I'm the Principal Investigator for this academic research study. I have carefully read every single message sent to our research team, and I am dismayed that the emails in our study came across as security risks or legal threats. The intent of our study was to understand privacy practices, not to create a burden on website operators, email system operators, or privacy professionals. I sincerely apologize. I am the senior researcher, and the responsibility is mine.

The touchstone of my academic and government career, for over a decade, has been respecting and empowering users. That's why I study topics like web tracking, dark patterns, and broadband availability, and that's why I launched this study on privacy rights. I aim to be beyond reproach in my research methods, both out of principle and because my work often involves critiquing powerful companies and government agencies. In this instance, I fell short of that standard. I take your feedback to heart, and here is what I am doing about it.

First, our team will not send any new automated inquiries for this study. We suspended sending on December 15, and that is permanent.

Second, our team is prioritizing a possible one-time follow-up email to recipients, identifying the academic study and recommending that they disregard the prior email. If that is feasible, and if experts in the email operator community agree with the proposal, we will send the follow-up emails as expeditiously as possible.

Third, I will use the lessons learned from this experience to write and post a formal research ethics case study, explaining in detail what we did, why we did it, what we learned, and how researchers should approach similar studies in the future. I will teach that case study in coursework, and I will encourage academic colleagues to do the same. While I cannot turn back the clock on this study, I can help ensure that the next generation of technology policy researchers learns from it.

Fourth, I will engage with the communities that have contacted me about this study, which have already offered valuable suggestions for future directions to simplify, standardize, and enhance transparency for GDPR and CCPA data rights processes. I very much appreciate the earnest outreach so far, and I will be reciprocating.

If you have questions or concerns about the study, please do not hesitate to reach out. I gratefully acknowledge the feedback that we have received.

Thank you for reading, and again, my sincere apologies.

Commonalities

Both: deception research

- Lying to / hiding information from subjects
    - Hypocrite commits: involuntary participation
    - CCPA spam: involuntary participation

Deception definition

*Deception is when a researcher **gives false information** to subjects or **intentionally misleads them** about some key aspect of the research. This could include feedback to subjects that involves creating false beliefs about oneself, one's relationship, or manipulation of one's self-concept.*

Incomplete Disclosure is a type of deception that involves withholding some information about the real purpose of the study, or the nature of the research procedures.

– https://research.oregonstate.edu/irb/research-involving-deception

Existing guidelines on deception research

- **Should be avoided** unless otherwise impossible

*”Ordinarily, research proposals failing to adhere to the principle of respect for persons by compromising the consent process **would not be approved**.“*
– *https://research.oregonstate.edu/irb/research-involving-deception*

- **Exceptions exist**

*”**in unique circumstances** where the study design requires omission of details that might alter the subject’s responses that are being investigated, vital information about the study or study activities can be withheld from subjects **until after their participation**.”*
– https://research.oregonstate.edu/irb/research-involving-deception

Standing on the shoulders of giants

Existing knowledge

- **Belmont report** (US, 1978)
  - Ethical principles for human subjects of research

- **Menlo report** (US DHS, Cyber Security Division, 2012)
  - Ethical framework for research involving ICT

Belmont report (1978)

- **3 principles:**
  - Respect for persons
  - Beneficience
  - Justice

- **Application:**
  - Informed consent
  - Assessment of risk and benefits
  - Selection of subjects

Menlo report (2012)

- **Respect for Persons**
- **Beneficence**
- **Justice**
- **Respect for Law and Public Interest**

Menlo report (2012)

- **Respect for Persons**
  - Participation as a research subject is voluntary, and follows from informed consent
  - Treat individuals as autonomous agents and respect their right to determine their own best interests
  - Respect individuals who are not targets of research yet are impacted
  - Individuals with diminished autonomy, who are incapable of deciding for themselves, are entitled to protection.

- **Beneficence**
  - Do not harm
  - Maximize probable benefits and minimize probable harms; Systematically assess both risk of harm and benefit.

Menlo report (2012)

- **Justice**
  - Each person deserves equal consideration in how to be treated, and the benefits of research should be fairly distributed according to individual need, effort, societal contribution, and merit
  - Selection of subjects should be fair, and burdens should be allocated equitably across impacted subjects.

- **Respect for Law and Public Interest**.
  - Engage in legal due diligence and be transparent in methods and results. Be accountable for actions.

APA guidelines on deception research

8.07 Deception in Research

a) Psychologists do not conduct a study involving deception **unless** they have determined that the **use** of deceptive techniques **is justified by** the study's **significant** prospective scientific, educational or applied **value and** that **effective nondeceptive alternative procedures are not feasible.**

APA guidelines on deception research

8.07 Deception in Research

a) Psychologists do not conduct a study involving deception **unless** they have determined that the **use** of deceptive techniques **is justified by** the study's **significant** prospective scientific, educational or applied **value and** that **effective nondeceptive alternative procedures are not feasible.**

b) Psychologists do not deceive prospective participants about research that is reasonably expected to cause physical pain or severe emotional distress.

APA guidelines on deception research

8.07 Deception in Research

a) Psychologists do not conduct a study involving deception **unless** they have determined that the **use** of deceptive techniques **is justified by** the study's **significant** prospective scientific, educational or applied **value and** that **effective nondeceptive alternative procedures are not feasible.**

b) Psychologists do not deceive prospective participants about research that is reasonably expected to cause physical pain or severe emotional distress.

c) Psychologists **explain any deception** that is an integral feature of the design and conduct of an experiment to participants **as early as is feasible**, preferably at the conclusion of their participation, but no later than at the conclusion of the data collection, and permit participants to withdraw their data.

Key takeaways

- **Guideline**

  if the study wouldn’t work without humans reacting/responding:
  it’s human subject research.

  - Requires approval (CETO)
  - Necessitates explanation: what is the approval about?
    - Privacy?
      - Well-trodden territory
    - Not privacy?
      - Help CETO avoid the trap of “no privacy violation”!

- Deception research: **avoid**.

Thanks for your attention and input!

S&P Panel on ethics video

- https://www.youtube.com/watch?v=JPdbl3sadrA