

Course Introduction

and some motivation

Mainack Mondal

CS 60081
Autumn 2024



Today's class

- Course logistics
- The story of usability
- Some case studies: *why* of usability in security / privacy

Instructors



- **Mainack Mondal:** usable security and privacy, system security and privacy, operationalizing privacy theories
 - Office: CSE 316

Website

<https://cse.iitkgp.ac.in/~mainack/courses/2024-autumn/usesec/>

IIT Kharagpur CS60081 Schedule

Usable Security and Privacy (CS60081) Autumn 2024

All secure and privacy-preserving systems are ultimately used by humans, who might or might not understand the intended usage of these systems. In fact, often users are the “last line of defense” in securing a system and if the systems are not designed keeping user mental model and their background knowledge in mind, that can lead to system misuse and consequent security and privacy disasters. Thus, only designing secure and private systems are not enough, we need to design secure and private systems keeping usability in mind. In other words, we need to understand the user expectation from the systems and incorporate this understanding in system design.

This course will focus on how to design for security and privacy in systems using a user-centric view. We will combine concepts from computer systems, human computer interaction (HCI) and secure/private system design. We will introduce core security and privacy technologies, as well as HCI techniques for conducting robust user studies. The course will cover topics like passwords, definitions of privacy, usable encryption, authentication, privacy of archival data, usability of crypto libraries and privacy notices. Keep an eye on the course [schedule](#) for details.

• • •

Course timings

- Credit : 3 – 0 – 0
- Wednesday 11:00 am - 12:00 pm
- Thursday 12:00 noon - 1:00 pm
- Friday 8:00 am to 9:00 am

Mode of teaching

- Offline lectures
 - Please come to the class (no recordings)
- (occasional) Pre-recorded lectures for special topics
 - We will upload the recorded lectures via MS teams
- Two exams + term project + 1 assignment + scribes
 - Quiz/viva/term project

MS teams

- Use the code cmbyl9a
 - Team name “Usable Security and Privacy 2024”

CSE Moodle

- All submissions will be via CSE moodle unless otherwise stated
 - Search in CSE Moodle for “CS60081: Usable Security and Privacy”
 - Use the key STUD4USP

Course evaluation: Exam

- Two Exams (approx. 60%)
 - Syllabus : Everything until that point
 - Dates will be in the webpage and announced in academic calendar

Course evaluation: Term project + Assignment + scribes

- 40% of the evaluation
 - Expected: You apply the knowledge gained from this class on a hands on practical problem
 - Write two reports/one presentation based on it
 - If interesting enough (and you wish) you can work after the course to make it a research paper submission
 - Talk to me
 - One assignment to practice knowledge of things you cannot do in term project – e.g., statistics

Course evaluation: Term project

- Requirements:
 - Submit periodic reports (via Moodle)
 - Give periodic presentations

Term project: reports

- Write in LaTeX/Word with ACM two column format
- Suggested: use overleaf/ Share point for collaboration

Term project: Next todo

- Will float the topics soon
- Have an idea on usable security/privacy you think you should work on?
- Already have group members?
- Talk to us ASAP (drop a private chat/email)

Course logistics

- Questions?

Ethical considerations



Source: <https://myozonelayer.com/2016/11/22/the-4th-monkey-do-no-evil/>

Ethical considerations

- Don't do evil
- If you feel its wrong, it is wrong
- Cyber offenses are punishable by law
 - The case of Mirai Botnet -- five years of probation, 2,500 hours of community service, and \$127,000 fine.
 - The case of Swatting – people got killed

Today's class

- Course logistics
- The story of usability
- Some case studies: *why* of usability in security / privacy



Lack of usable security costs billions

- 2019: UK's Information Commissioner's Office (ICO)

“90% of cyber data breaches were caused by user error last year”

Without usability no effective security

- 2009: Department of Homeland Security (DHS) published a list of "hard problems in INFOSEC Research", 11th problem was "Usable security"
- "Security must be usable by persons ranging from nontechnical users to experts and system administrators. Furthermore, systems must be usable while maintaining security. In the absence of usable security, there is ultimately no effective security."

Understanding how would users behave

- 2008: National Academy of Engineering, US
Published “Grand Challenges of Engineering”

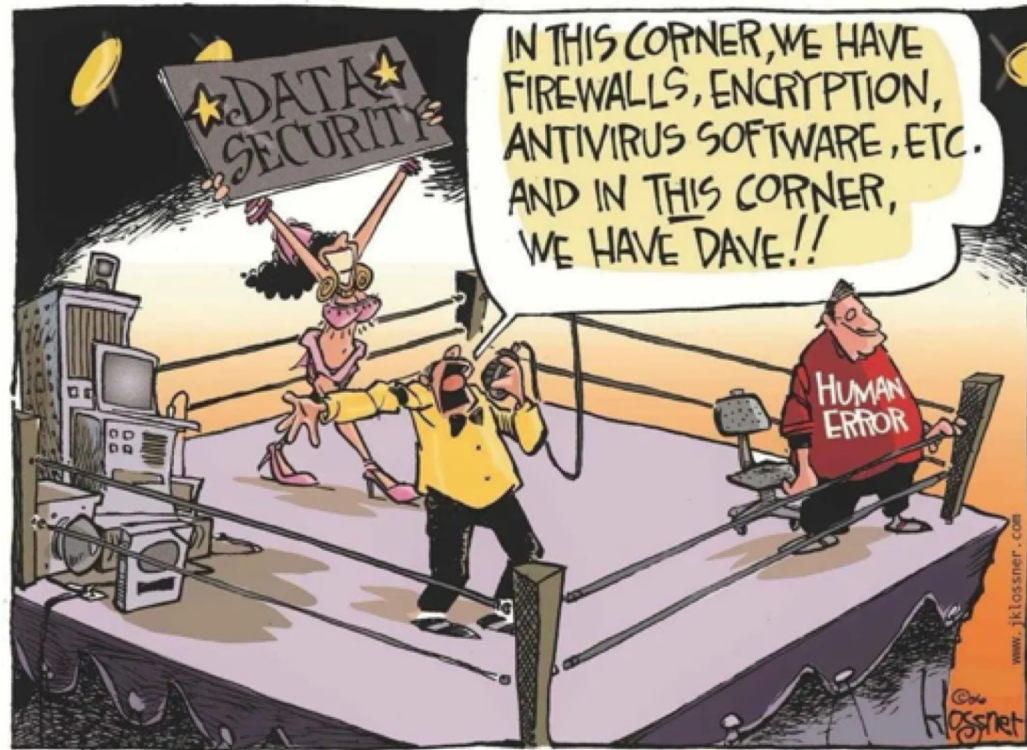
”one of the needs to “secure cyberspace” was to understand how the psychology of computer users can “increase the risk of cybersecurity breaches”

Humans are important in security

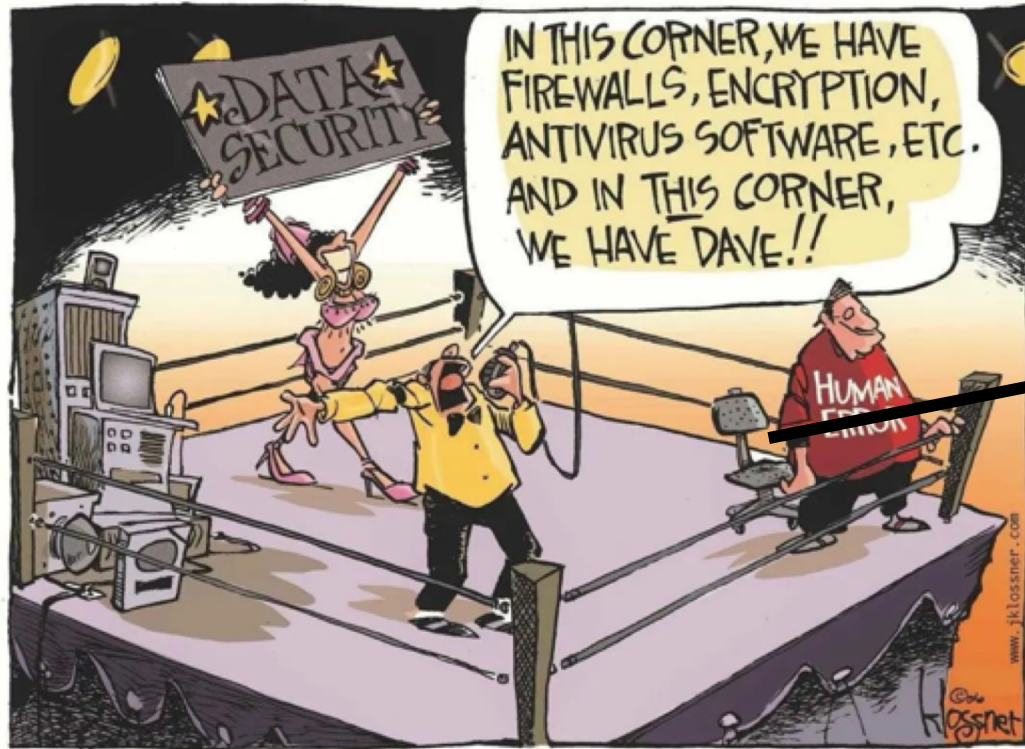
“Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations... But they are sufficiently pervasive that we must design our protocols around their limitations.”

-- C. Kaufman, R. Perlman, and M. Speciner Network Security: PRIVATE Communication in a PUBLIC World. 2nd edition. Prentice Hall, page 237, 2002.

Why humans



Why humans



~~Human
behavior~~

The human threat

- Malicious humans
- Clueless humans
- Unmotivated humans
- Humans constrained by human limitations

Humans are the weakest link

In practice

“Given a choice between dancing pigs and security, users will pick dancing pigs every time”

-- Edward Felten

Experiment on the weakest link

- The U.S. Department of Homeland Security ran a test in 2011 to see how hard it was for hackers to corrupt workers and gain access to computer systems:
- staff **secretly dropped computer discs and USB thumb drives** in the parking lots of government buildings and private contractors.
- Of those who picked them up: **60 percent plugged the devices into office computers**
- If the drive or CD case had an official logo, 90 percent were installed.

Security and usability

- If a system is secure but not usable
 - User will move to usable (even insecure) systems
- If a system is usable but insecure
 - It will get compromised – can not last long
- When trying to make secure systems usable, we add complexity. Complexity leads to higher chances to doing something wrong, i.e. less secure!

Systems are not good enough

Password:

Systems are not good enough

Password:	<input type="text" value="password"/>
Password:	<input type="text" value="password"/>
Hide:	<input type="checkbox"/>
Score:	<div style="background-color: #ff4500; color: white; padding: 2px; display: inline-block;">8%</div>
Complexity:	Very Weak

Systems are not good enough

Password:	<input type="text" value="password"/>
------------------	---------------------------------------

Password:	<input type="text" value="password"/>
Hide:	<input type="checkbox"/>
Score:	<div style="background-color: #ff4500; color: white; padding: 2px; text-align: center;">8%</div>
Complexity:	Very Weak

Password:	<input type="text" value="password"/>	<ul style="list-style-type: none">• Minimum 8 characters in length• Contains 3/4 of the following items:<ul style="list-style-type: none">- Uppercase Letters- Lowercase Letters- Numbers- Symbols
Hide:	<input type="checkbox"/>	
Score:	<div style="background-color: #ff4500; color: white; padding: 2px; text-align: center;">8%</div>	
Complexity:	Very Weak	

Systems are not good enough

Password:	<input type="text" value="password"/>
------------------	---------------------------------------

Password:	<input type="text" value="password"/>
Hide:	<input type="checkbox"/>
Score:	<div style="width: 8%; background-color: orange; text-align: center;">8%</div>
Complexity:	Very Weak

Password:	<input type="text" value="password"/>	<ul style="list-style-type: none">• Minimum 8 characters in length• Contains 3/4 of the following items:<ul style="list-style-type: none">- Uppercase Letters- Lowercase Letters- Numbers- Symbols
Hide:	<input type="checkbox"/>	
Score:	<div style="width: 8%; background-color: orange; text-align: center;">8%</div>	
Complexity:	Very Weak	

Password:	<input type="text" value="p@\$w0rd!"/>	<ul style="list-style-type: none">• Minimum 8 characters in length• Contains 3/4 of the following items:<ul style="list-style-type: none">- Uppercase Letters- Lowercase Letters- Numbers- Symbols
Hide:	<input type="checkbox"/>	
Score:	<div style="width: 86%; background-color: green; text-align: center;">86%</div>	
Complexity:	Very Strong	

Systems are not good enough

Password:	<input type="text" value="password"/>
Hide:	<input type="checkbox"/>
Score:	<div style="width: 8%; background-color: orange; text-align: center;">8%</div>
Complexity:	Very Weak

<http://www.passwordmeter.com/>

Password:	<input type="text" value="password"/>	<ul style="list-style-type: none">• Minimum 8 characters in length• Contains 3/4 of the following items:<ul style="list-style-type: none">- Uppercase Letters- Lowercase Letters- Numbers- Symbols
Hide:	<input type="checkbox"/>	
Score:	<div style="width: 8%; background-color: orange; text-align: center;">8%</div>	
Complexity:	Very Weak	

Password:	<input type="text" value="p@\$w0rd!"/>	<ul style="list-style-type: none">• Minimum 8 characters in length• Contains 3/4 of the following items:<ul style="list-style-type: none">- Uppercase Letters- Lowercase Letters- Numbers- Symbols
Hide:	<input type="checkbox"/>	
Score:	<div style="width: 86%; background-color: green; text-align: center;">86%</div>	
Complexity:	Very Strong	

Security & Privacy

(CCS, Usenix Security, IEEE S&P, NDSS)

+

Human-Computer Interaction

(CHI, UbiComp, CSCW)

=

Usable Security and Privacy

(PETS, SOUPS)

Today's class

- Course logistics
- The story of usability
- Some case studies: *why* of usability in security / privacy

Case study 1: Passphrases

- "A memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity." -- NIST

correct-horse-battery-staple

spindle-chemicals-griminess-waviness

sponge-bob-square-pants

rub-revisions-lilo-clark-apple-betting

Case study 1: Passphrases

- "A memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity." -- NIST

correct-horse-battery-staple

spindle-chemicals-griminess-waviness

sponge-bob-square-pants

rub-revisions-lilo-clark-apple-betting

Case study 1: Passphrases

- "A memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity." -- NIST

Passphrases have a usability tradeoff

User-generated word sequence are **easy to remember**, **easy to guess**

System-generated random word sequences: **hard to remember**, **hard to guess**

Most of prior work on usable passphrase **sought user intervention**

Case study 1: Passphrases

- "A memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity." -- NIST

Passphrases have a usability tradeoff

User-generated word sequence are **easy to remember**, **easy to guess**

System-generated random word sequences: **hard to remember**, **hard to guess**

Most of prior work on usable passphrase **sought user intervention**

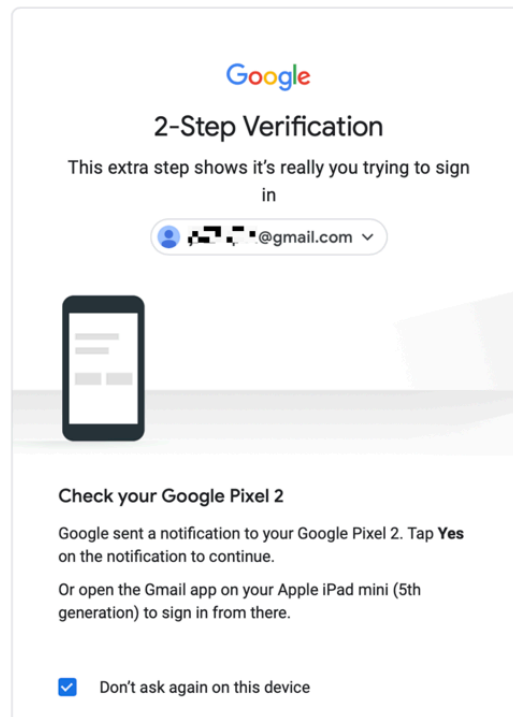
**Usability Need: Automatically generate passphrases
which balances both memorability and security**

Case study 2: Two-factor authentication

- What is 2-factor authentication?
 - Factor 1: What you know (e.g., your password)
 - Factor 2: What you have (e.g., OTP on your phone)

Case study 2: Two-factor authentication

- What is 2-factor authentication?
 - Factor 1: What you know (e.g., your password)
 - Factor 2: What you have (e.g., OTP on your phone)



Case study 2: Two-factor authentication

- Problems?
 - User's time it takes increase and attention
 - Losing device – breaking phone

Case study 2: Two-factor authentication

- The story of a Philadelphia librarian
 - Old, often homeless people use public libraries for internet
 - The computers wipe all session information once logged out
 - Every time Gmail ask for two-factor
 - That's good, right? More secure?

Case study 2: Two-factor authentication

- The story of a Philadelphia librarian
 - Old, often homeless people use public libraries for internet
 - The computers wipe all session information once logged out
 - Every time Gmail ask for two-factor
 - That's good, right? More secure?
 - **NO**

Case study 2: Two-factor authentication

- The story of a Philadelphia librarian

it is very common for poor working-class people to have their cellular service shut-off due to a missed payment on their phone bill. Often, they have had to sell their phone to make rent, or their phone has been stolen or broken and they cannot afford a new one and when they do finally get a new one **they are unable to get their old phone number transferred over.**

Case study 2: Two-factor authentication

- The story of a Philadelphia librarian

it is very common for poor working-class people to have their cellular service shut-off due to a missed payment on their phone bill. Often, they have had to sell their phone to make rent, or their phone has been stolen or broken and they cannot afford a new one and when they do finally get a new one they are unable to get their old phone number transferred over.

- So?

Case study 2: Two-factor authentication

- The story of a Philadelphia librarian

it is very common for poor working-class people to have their cellular service shut-off due to a missed payment on their phone bill. Often, they have had to sell their phone to make rent, or their phone has been stolen or broken and they cannot afford a new one and when they do finally get a new **one they are unable to get their old phone number transferred over.**

When this happens, **patrons are locked out of their accounts, sometimes permanently, with no support line to turn to...**an old woman came in to print out paystubs from her email that she needed in order to re-certify her income for her subsidized housing. The certification was due by the end of the day. **Because she did not have her old phone and phone number, we were completely unable to get her back into her email.**

If she does not recertify her income, she could lose her low-income housing. This elderly woman, looked to be in her 70s, might lose the roof over her head, due to being unable to log into her Google account, because she lost her old phone and with it, her phone number.

Case study 2: Two-factor authentication

- Full story (and her open letter) here:
<https://docs.google.com/document/d/1f6HPQbUjslcbjVHkJkAgYmQmBV3PRRHEcx4WL5rxuE8/preview>
- Strict two factor is for people who can afford a phone and afford to keep a sustained connection
 - Hurts the poor who perhaps need access most

Case study 3: Encrypting emails

- What is encryption?

Case study 3: Encrypting emails

- What is encryption?
 - The art of hiding information so that only intended recipient can read



Case study 3: Encrypting emails

- How many of you use it to send emails?

Case study 3: Encrypting emails

- How many of you use it to send emails?



tools to send encrypted emails



All

Videos

Shopping

Images

News

More

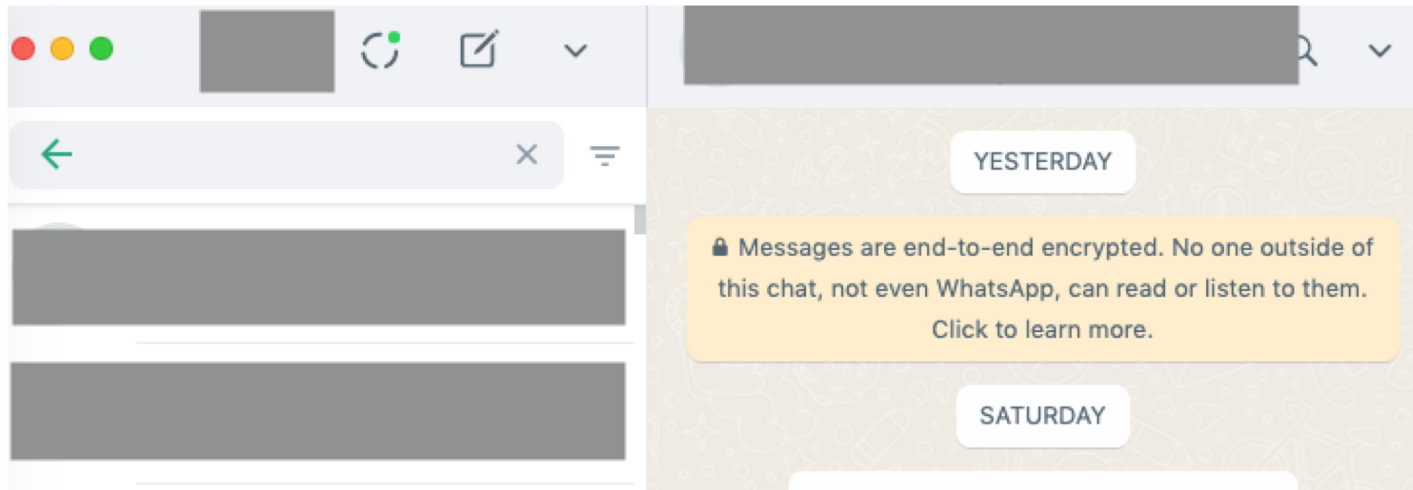
Tools

About 23,800,000 results (0.54 seconds)

- Why so low?

Case study 3: Encrypting emails

- Current way you use encryption



Case study 3: Encrypting emails

- Current way you use encryption



  <https://www.onlinesbi.com>

- In this case to ensure usability, the software proactively generate key and encrypt/decrypt

Case study 4: Cookie banners

- What are cookie banners?

Case study 4: Cookie banners

- What are cookie banners?

Your tracker settings



We use cookies and similar methods to recognize visitors and remember their preferences. We also use them to measure ad campaign effectiveness, target ads and analyze site traffic. To learn more about these methods, including how to disable them, [view our Cookie Policy](#).

Starting on July 20, 2020 we will show you ads we think are relevant to your interests, based on the kinds of content you access in our Services. You can [object](#). For more info, see our [privacy policy](#).

By tapping 'accept,' you consent to the use of these methods by us and third parties. You can always change your

ACCEPT

REJECT

Case study 4: Cookie banners

- What are cookie banners?

Your tracker settings



We use cookies and similar methods to recognize visitors and remember their preferences. We also use them to measure ad campaign effectiveness, target ads and analyze site traffic. To learn more about these methods, including how to disable them, [view our Cookie Policy](#).

Starting on July 20, 2020 we will show you ads we think are relevant to your interests, based on the kinds of content you access in our Services. You can [object](#). For more info, see our [privacy policy](#).

By tapping 'accept,' you consent to the use of these methods by us and third parties. You can always change your

ACCEPT

REJECT

Accept the updated privacy & cookie policy

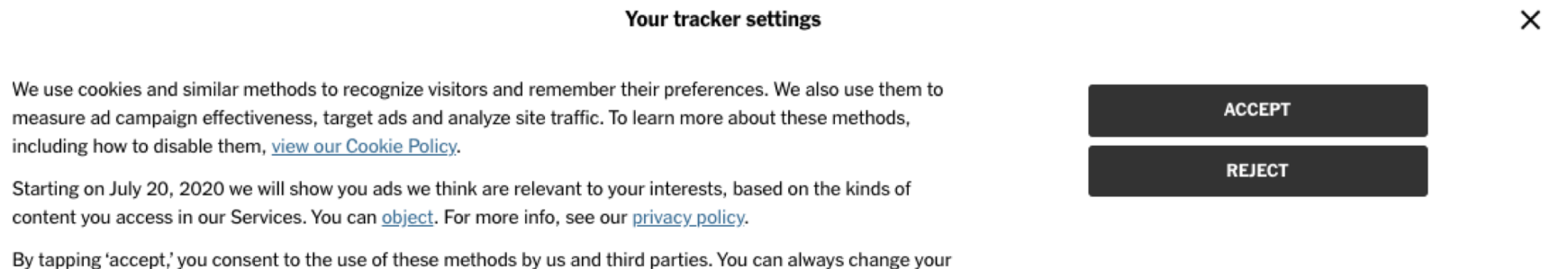
We use cookies and other tracking technologies to provide services in line with the preferences you reveal while browsing the Website to show personalize content and targeted ads, analyze site traffic...[Read more](#)

I agree to see customized ads that are tailor-made to my preferences

Accept

Case study 4: Cookie banners

- What are cookie banners?



Your tracker settings ✕

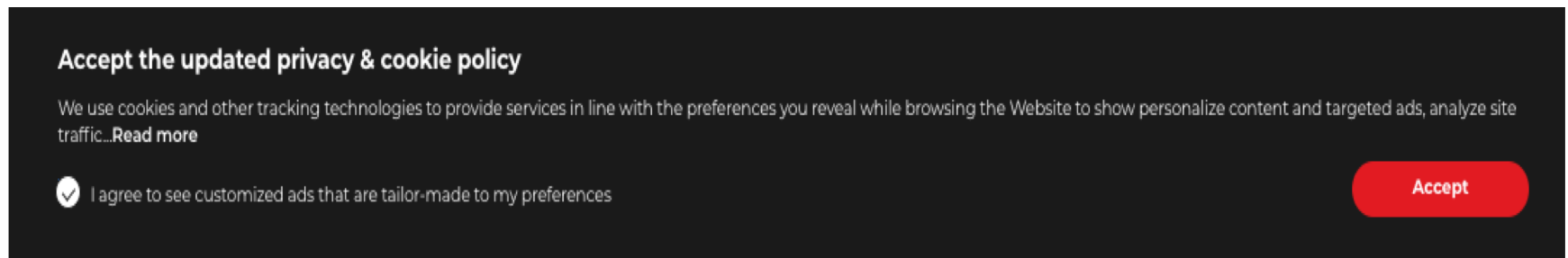
We use cookies and similar methods to recognize visitors and remember their preferences. We also use them to measure ad campaign effectiveness, target ads and analyze site traffic. To learn more about these methods, including how to disable them, [view our Cookie Policy](#).

Starting on July 20, 2020 we will show you ads we think are relevant to your interests, based on the kinds of content you access in our Services. You can [object](#). For more info, see our [privacy policy](#).

By tapping 'accept,' you consent to the use of these methods by us and third parties. You can always change your

ACCEPT

REJECT



Accept the updated privacy & cookie policy

We use cookies and other tracking technologies to provide services in line with the preferences you reveal while browsing the Website to show personalize content and targeted ads, analyze site traffic...[Read more](#)

I agree to see customized ads that are tailor-made to my preferences

Accept

- Just having a cookie banner is not enough for privacy

Case study 5: Healthcare privacy

Case study 5: Healthcare privacy



Case study 5: Healthcare privacy

Kokilaben Dhirubhai
hospital & medical research
Every

INTRODUCES
RAPIDA
AI

FIRST IN MUMBAI AND WESTER

RAPIDA AI

Products & Solutions Comp

Faster Triage & Transfer Decisions Based on CT Imaging

The only, premiere, FDA-approved AI-based medical device that determines suspicion of ICH and LVO based on non-contrast CT (NCCT) imaging. Rapid NCCT Stroke's triage and notification algorithm

Case study 5: Healthcare privacy



RAPIDAI

Products & Solutions Comp

FIRST

Apollo Hospitals has launched an automated AI based real-time rapid-response patient monitoring system, Enhanced Connected Care.

POSTED BY APOLLO HOSPITALS | 11 OCT,2022

Case study 6: IoT surveillance (CCTV)

Case study 7: State of ERP security

Case study 8: ChatGPT / AI