

Privacy Rights and Confidentiality in the Digital Era and Technology and Tools for Secure Communication

AORC – Cybersecurity Awareness


Presenter: Prof. Manoj Maharaj

Date: 10 October 2023

A large, solid red circle is positioned on the left side of the slide, partially cut off by the edge.

Introduction

CIA is critical for most information, but more so for the legal profession

A decorative graphic consisting of four thick, purple, curved dashes arranged in a curved path in the bottom right corner of the slide.

Data – at the heart of the modern enterprise

Every digital interaction generates vast amounts of data. This data, while invaluable for enhancing user experiences and optimizing services, is also a treasure trove for malicious actors.

Sources of Data Collection

- Social Media Interactions
- E-Commerce Platforms
- Health and Fitness Apps
- Smart Home Devices



Implications of this Data

- Banks can see your social media posts to ascertain your credit worthiness
 - Insurer may use posts to deny claims
 - Employer may use social media before making a job offer
-



Right To Privacy

- All countries protect privacy rights to some level
- This does not prevent criminal exploitation – especially cross-border
- You need to ensure your own privacy protection



Knowledge and Awareness

The end-user needs to be educated about what is possible to be able ensure protection

There are certainly benefits – personalized healthcare, personalized shopping, ...

If you are a data custodian this issue is much more pressing.

The Dark side of Data Collection

- Data Brokers
- Unauthorised Data Access
- Surveillance Capitalism: Shoshana Zuboff describes the monetisation of personal data through surveillance. The user becomes the product (think of the Truman Show Movie)



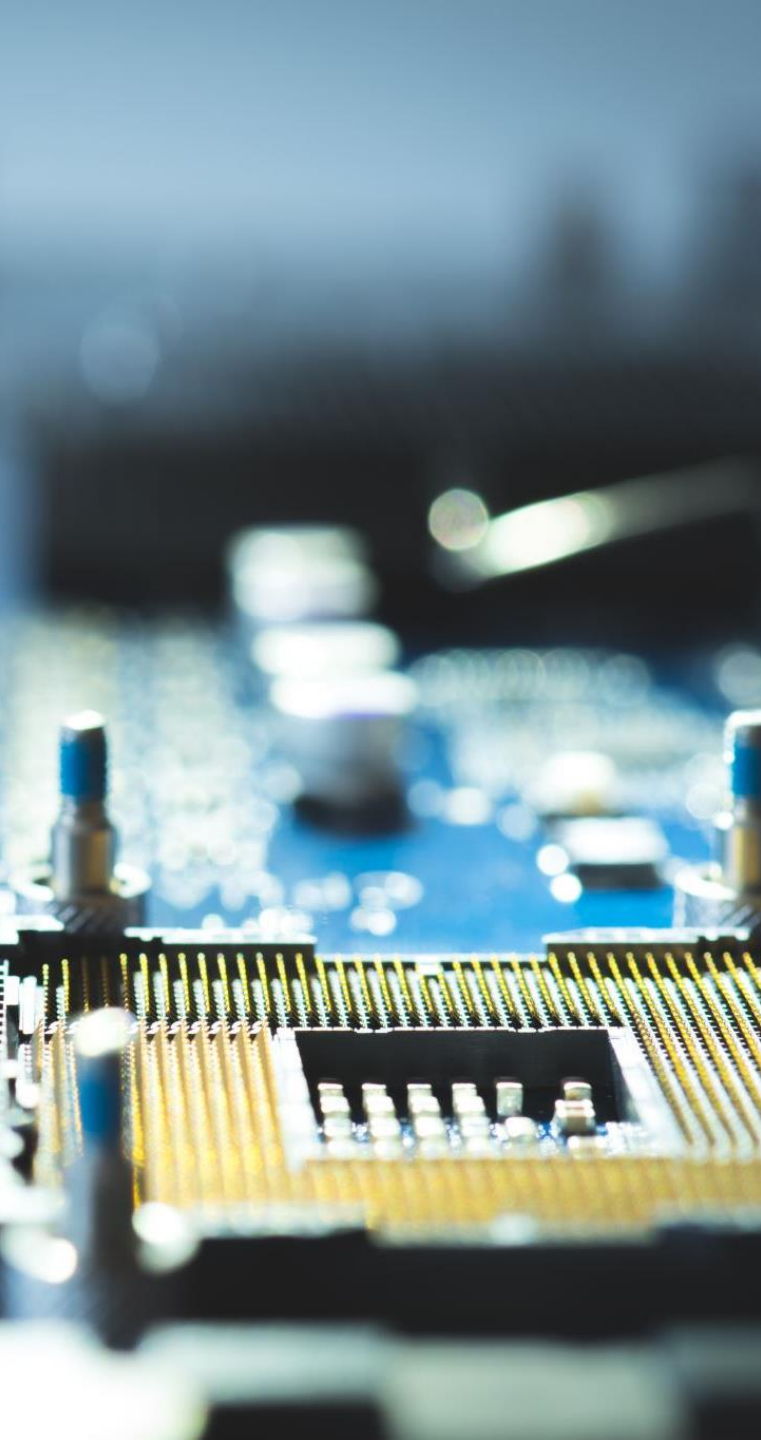
Challenges in Secure Communication

- Challenges include
 - third-party risks,
 - outdated technology,
 - human error
 - technophobia
 - Lack of knowledge



Encryption: The Backbone of Secure Communication

- Encryption is the process of converting plaintext into an unreadable format, decipherable only with a unique key.



Tools for Secure Communication

- End-to-End Encrypted Messaging Platforms
- Secure Email Services
- Virtual Private Networks (VPNs)
- Secure File Storage and Sharing Solutions
- Two-Factor Authentication (2FA)
- Secure Video Conferencing Tools
- Digital Signature Services

Phishing: The Primary Vector for Hackers

- Phishing involves tricking individuals into revealing sensitive information, such as passwords. This is the primary method hackers use to breach secure communications.



Some Examples

The Fake Invoice

- Click on a link to review the invoice!

Urgent request from the Boss

- Request for funds transfer, or client information

Request for account verification

- Verify account or update password via a link

Important legal documents to preview

- Click on attachment to review the docs

Tax refund email

- Link to tax authority for verification

'Friend' message on social media

- Link to message

Best Practices for Avoiding Phishing Attacks

Awareness

Strong, unique passwords

Use 2FA

Verify unexpected requests

Do not use public WiFi

Monitor account activity

Take advice from experts – they know what they are talking about

Learn how to use digital signatures

Share and discuss with each other

Conclusion

This is a short talk designed to make you aware – at a very high-level of what threats you face and what is available to mitigate them.

Seek out training opportunities

Remember that cybersecurity is not only about your workplace but about your personal and family life as well.

Q&A