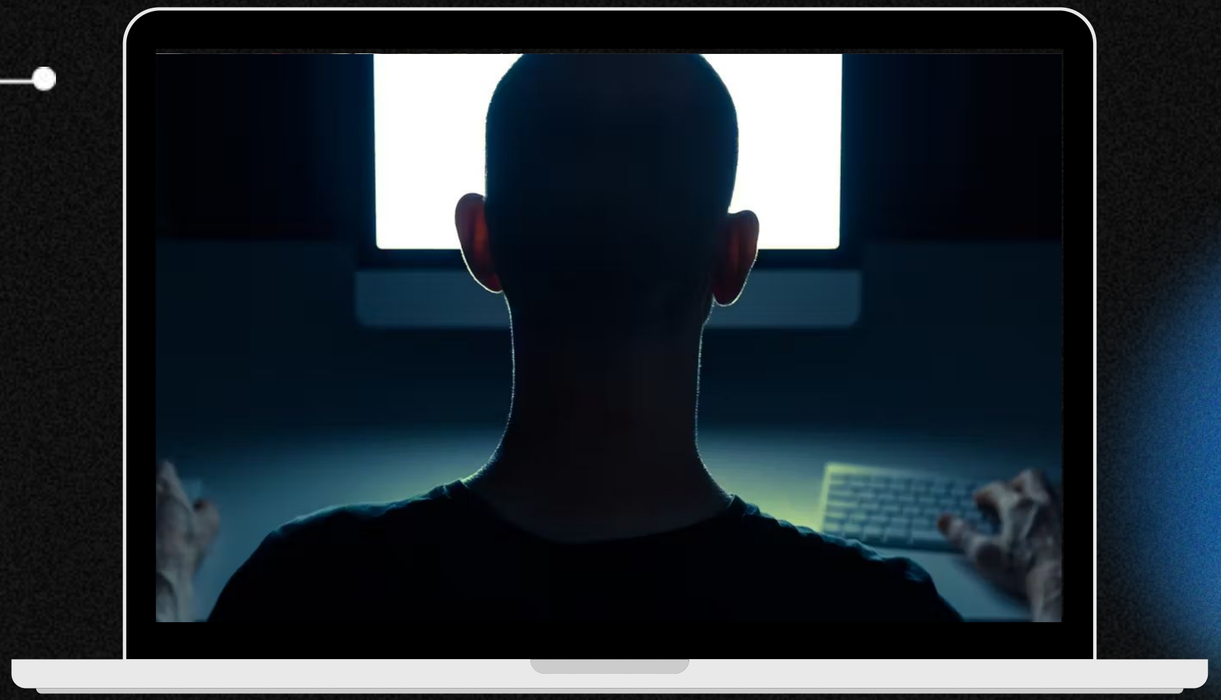
WHOIS Data & Post-GDPR Domain Privacy

SHREYA SHIVAKUMAR
ICANN82 NEXTGEN

Privacy:
A Double-Edged Sword?



01.

WHOIS Data

- WHOIS asks and retrieves information about the registration of a domain name or Internet Protocol (IP) address
- WHOIS lookup is used to retrieve generic top-level domain (gTLD) registration data
- "Thick" WHOIS data poses more privacy concerns than "thin" WHOIS data

WHOIS & Data Privacy

WHOIS data has proven instrumental to law enforcement activities, including combating cybercrime, IP infringement, and child sexual exploitation.

Some privacy advocates have opposed making gTLD registration data publicly available via the WHOIS database, stating that users do not give affirmative consent to publish their information online.

Diverse Stakeholders

Domain Name Companies

GoDaddy

Privacy Rights Organizations

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Law Enforcement

GDPR

02.

The General Data Protection Regulation (GDPR) is a European Union (EU) data protection regulation. It protects the data privacy of anyone within EU borders, and applies to any organization that processes the personal data of EU residents.

Before GDPR

New domains are registered in the WHOIS database and include owner information, such as email, phone, and physical address. Criminals frequently reuse the same registration data—even if it's fake—because it's cheaper and more efficient. Investigators use this information to help determine legitimacy of websites. Machine automation correlates domains registered with the same contact information, enabling filters to quickly block all related domains.

With GDPR, This May Change

GDPR mandates that personal information cannot be shared or published without the owners' permission. This means security professionals will no longer have fast access to the data in the WHOIS database, such as the domain owners' name, email and phone number.

✓ Many domains are blocked at once		✗ Difficult to identify attack source
✓ Fewer malicious emails		✗ Increase in malicious emails
✓ Attack cycle shortened		✗ Extended attack timeline

ICANN's Temporary Specification for gTLD Registration Data

Data Collection

Registrars were allowed to continue to collect registration data from domain owners

Tiered Access Model

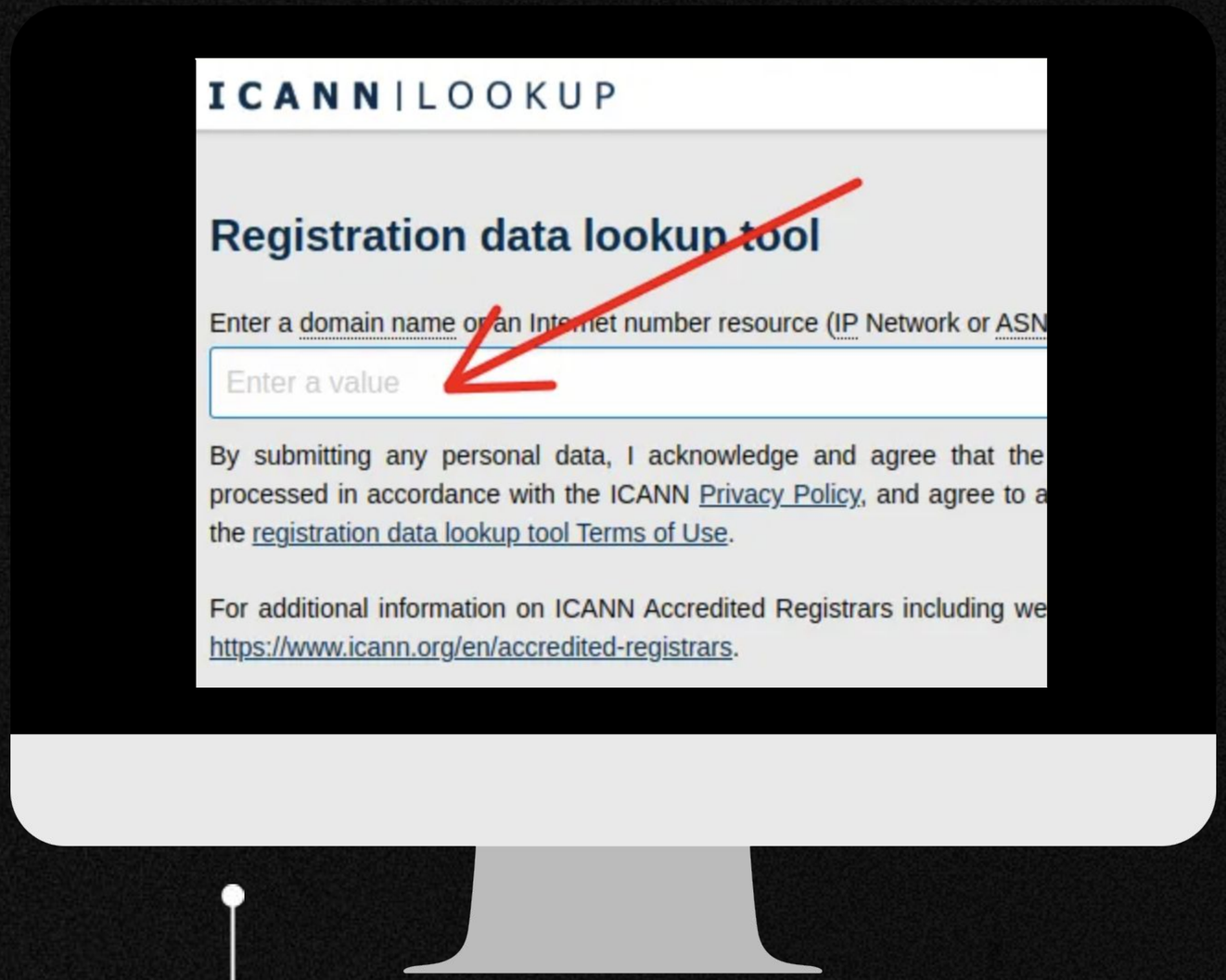
Mandated that registrars put up a generic email address or an online contact form

Request System

Users with legitimate interests request access to WHOIS data through Registrars and Registry Operators

Means of Contact

Mandated that registrars put up a generic email address or an online contact form



RDAP

The Registration Data Access Protocol (RDAP) allows for tiered access to gTLD registration data, enabling registrars to disclose personal information only to authorized parties

Future Opportunities & Challenges for Domain Privacy

— Questions?