Demystifying the Privacy Landscape for the Cybersecurity Professional
Ken leads Lowenstein Sandler’s information security and data privacy programs. He has more than 20 years of experience implementing and supporting secure, complex information technology infrastructures. Ken’s detailed knowledge of security and network methodologies, techniques, and best practices enables him to thoroughly assess and remediate cybersecurity threats and vulnerabilities.

He is President of the New Jersey Chapter of (ISC)$^2$, and is also a member of the Executive and Threat Intelligence Committees of the Legal Services Information Sharing and Analysis Organization (LS-ISAO), a member-driven community providing a secure framework for sharing actionable threat intelligence and vulnerability information.

Ken is a volunteer with the Cybersecurity Workforce Alliance (CWA), which mentors high school and college students who are breaking into the cybersecurity field.

He hold several cybersecurity and privacy certifications including the CISSP, CIPP/US, CIPT, CIPM, CISM and CCSP.
Agenda

1. Why should I care?
2. How did we get here?
3. Understanding the Privacy landscape
4. What types of jobs are available?
5. What resources are there?
WHY SHOULD I CARE?

Privacy laws are gaining ground in the U.S. and around the world

Many cybersecurity officers need to be responsible for privacy as well

Heavy fines and/or penalties for non-compliance

Privacy cannot exist without adequate security

It is one of the fastest growing fields in the U.S.
HOW PRIVACY COULD IMPACT A CYBERSECURITY PROFESSIONAL

1. A customer/client requests to be removed from your systems
2. Backups are restored that have customer info that was already removed from your systems
3. A web form requests personal info without explaining why they need it or who has access to it
4. Development is outsourced to third-parties, who use personal data when testing
5. Cookies are tracking more information than what your privacy notification states
6. Your company has decided to enter a new market in another region
7. Time card systems uses biometrics
**How Did We Get Here?**

1995
- European Data Protection Directive was created

2000
- Safe Harbor Agreement was created between EU and US

2001
- Patriot Act was created in response to 9/11

2013
- Snowden released intel about global surveillance programs

2015
- Safe Harbor Agreement was ruled invalid

2016
- Privacy Shield was created to replace Safe Harbor

2018
- General Data Protection Regulation (GDPR) was enforced

2020
- Privacy Shield was ruled invalid and Patriot Act expired
COUNTRIES WITH COMPREHENSIVE PRIVACY LAWS
CYBERSECURITY TRIAD AND THE NIST CSF FUNCTIONS

Availability
Confidentiality
Integrity

Identify  Detect  Protect  Respond  Recover
PRIVACY TRIAD AND THE NIST PRIVACY FRAMEWORK FUNCTIONS

Accuracy

Identify  Govern  Control  Communicate  Protect

Accessibility

Confidentiality of Personal Data

Accuracy
WHY CYBERSECURITY IS AN ESSENTIAL PART OF PRIVACY

Cybersecurity Risks:
- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

Cybersecurity-related privacy events:
- PROTECT-P
- DETECT
- RESPOND
- RECOVER

Privacy Risks:
- IDENTIFY-P
- GOVERN-P
- CONTROL-P
- COMMUNICATE-P
### Taxonomy Challenges Within Privacy Laws

<table>
<thead>
<tr>
<th>HIPAA</th>
<th>GDPR</th>
<th>CCPA</th>
<th>VCDPA/CPA</th>
<th>In Plain English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered Entity</td>
<td>Controller</td>
<td>Business</td>
<td>Controller</td>
<td>The Company Who Is Responsible For Your Data</td>
</tr>
<tr>
<td>Business Associate</td>
<td>Processor</td>
<td>Service Provider</td>
<td>Processor</td>
<td>Vendors That Were Given Permission to Process Your Data</td>
</tr>
<tr>
<td>Individual</td>
<td>Data Subject</td>
<td>Consumer</td>
<td>Consumer</td>
<td>You</td>
</tr>
</tbody>
</table>
### WHAT DATA SHOULD I BE CONCERNED ABOUT?

<table>
<thead>
<tr>
<th>Personally Identifiable Information (PII)</th>
<th>Protected Health Information (PHI)</th>
<th>Personal Data (GDPR)</th>
<th>Sensitive Data (GDPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSN#</td>
<td>Medical Records</td>
<td>Online identifiers</td>
<td>Race / ethnic origin</td>
</tr>
<tr>
<td>Email address</td>
<td>Medical Billing Information</td>
<td>Biometrics</td>
<td>Trade-union membership</td>
</tr>
<tr>
<td>Phone number</td>
<td>Health Insurance</td>
<td>Video surveillance</td>
<td>Sex life or sexual orientation</td>
</tr>
<tr>
<td>Drivers license</td>
<td></td>
<td>Potentially any information that relates to an identifiable person</td>
<td>Political opinions</td>
</tr>
<tr>
<td>Bank account number</td>
<td></td>
<td>Data obtained directly or indirectly</td>
<td>Religious beliefs</td>
</tr>
</tbody>
</table>
COMMON PRIVACY PRINCIPLES

Notice
What data is used, how it is used and the purpose for collecting. Should be transparent

Choice and Consent
Right to opt-in / opt-out. Data should not be given to third-parties without consent

Access and Participation
Access rights and control of data from owners

Relevancy
Is the data being used for its original purpose and should be obtained lawfully

Enforcement
Owners or custodians of data should be held accountable

Security and Accuracy
Are adequate safeguards in place
# COMMON INDIVIDUAL PRIVACY RIGHTS

<table>
<thead>
<tr>
<th>Data Subject Rights</th>
<th>In Plain English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to be informed</td>
<td>What are they doing with my data and are other companies using it?</td>
</tr>
<tr>
<td>Right to access</td>
<td>Can I see my data?</td>
</tr>
<tr>
<td>Right to rectification</td>
<td>Can they fix my data if it’s wrong?</td>
</tr>
<tr>
<td>Right to erasure</td>
<td>Can I have them erase my data?</td>
</tr>
<tr>
<td>Right to data portability</td>
<td>Can I have my data?</td>
</tr>
<tr>
<td>Right to object</td>
<td>Can I object that they have my data?</td>
</tr>
<tr>
<td>Right to restrict processing</td>
<td>Can I stop them from using my data?</td>
</tr>
<tr>
<td>Personal data breach rights</td>
<td>Can I be notified if my data is stolen?</td>
</tr>
<tr>
<td>Right to avoid automated decision-making</td>
<td>Can they stop having a computer determine if I qualify for a loan?</td>
</tr>
</tbody>
</table>
NO CONSENSUS ON CYBERSECURITY FRAMEWORKS

ISO 27001:2013

CIS Controls

CYBERSECURITY FRAMEWORK VERSION 1.1

NIST
National Institute of Standards
Special Publication 800-53
How Do I Start Developing a Privacy Program?

1. Determine scope of assessment and understand your regulatory requirements and client/customer obligations
2. Inventory your data that is in scope
3. Identify the inherent privacy risks of your organization
4. Perform a Privacy Impact Assessment on each system or database
5. Develop Gap Assessment and Risk Register identifying the necessary preventive and corrective controls to implement
WHAT NON-LAWYER PRIVACY JOBS ARE AVAILABLE?

Career Positions in Privacy

- CONSULTANT
- ANALYST
- ENGINEER
- PROGRAM MANAGER
- GRC
PRIVACY RESOURCES

• IAPP – Conferences, Meetups, Newsletters, Certifications, Podcasts
• NIST Privacy Framework
• ISO 27701 Privacy Framework
• Webinars from OneTrust and TrustArc
• CPO Magazine
• LinkedIn
• Blogs from law firms that have privacy practices
KEY TAKEAWAYS

➢ The privacy field isn’t just for lawyers
➢ Tremendous momentum in protecting an individual’s privacy rights is happening throughout the world
➢ It is a very dynamic field that is evolving quickly
➢ More cybersecurity professionals are needed to understand the privacy landscape
Any Questions