Secret Squirrels and Flashlights: Legal Risks and Threat Intelligence

Cristin Flynn Goodwin
Assistant General Counsel | Customer Security & Trust
Whois?

I'M LIKE TOTALLY A LAWYER
Disclaimer

This presentation does not constitute legal advice.

If you work for Microsoft, come talk to me later.
Then it’s legal advice.
Maturing With Intent
It’s all about your (Company’s) information

Generated by your company

Acquired from your customers or their use of your products or service

Shared formally under an agreement with private sector or government partners

Shared informally under TLP

Compelled by law enforcement

Acquired by purchase

Open source
Legal Risks in TI

Information Sharing
Sharing with Government
Incident Response
Successful Disruptions
Create a principled approach to sharing

Identify data you have relative to risk (high / medium / low) and what can always be shared

Think about tools you use to share (Slack, Signal, Teams)

Think about the value of the exchange and benefit to the company
Sidebar: Traffic Light Protocol

For governments, cannot circumvent law, Executive Order, agency regulation, or other executive mandates.

In private sector, TLP struggles against contractual commitments to maintain confidentiality.
Working with the US Government

All government employees have basic obligations of public service:

- Cannot bind gov’t without authorization
- Cannot give preferential treatment to private organizations or individuals
- Cannot appear to violate the law or ethics
Sharing with the US Government

Cyber threat indicators and defensive measures provided to the federal government can be disclosed, retained, and used by any federal agency or department for:

- A cybersecurity purpose;
- The purpose of identifying a cybersecurity threat, including the source of such a cybersecurity threat or a security vulnerability;
- Other serious harms regarding risk of death, bodily injury, economic harm, or threats to children.
Engaging with Other Government Agencies

Authorities of the Agency matter
Laws versus Policies
DHS and NSA
Regulatory Agencies
Congress

IMAGINE HAVING TO WRITE OUT EVERY SINGLE TWEET
Engaging with Law Enforcement

“I have a contact at that Field Office”

All law enforcement action is governed by law, administrative policy / guidelines

The government can be forced to disclose the identity of confidential sources or the contents of their communications
Sidebar: Attorney Client Privilege

Whose data is it?

Can it leave the company?

When can a company be compelled to disclose privileged material?
Incident Response

Call your lawyers 😊

Understand whose incident it is – customer, company, third party – and the rights and obligations around that

Leverage your info sharing principles when under stress

Stick to the facts
Sidebar: Attribution

How is the law thinking about attribution?

What happens if attribution is incorrect?

Maturing Attribution to consider standards and policies – even a CVE-like process to make it easier to understand.
Successful Nation-State Disruptions

Legal framework for sharing or interacting with partners with clear roles and responsibilities

Need clear principles guiding all actions

Anticipate subpoenas; leverage ACP with intention
Microsoft’s Disruptions

4 nation-state legal disruptions

- Thallium
- Strontium
- Phosphorous
- Barium

Technical Disruption

- Zinc
In Conclusion

Make your lawyer a member of your TI team. That way when you call them, they know how to respond.
Thank You

Please stay in touch!  @CristinGoodwin