View this email in your browser

Legal Considerations When Gathering Online Cyber Intelligence Threats & Purchasing Data From Illicit sources

08/03/2020

Recently the US Department of Justice Cybersecurity Unit published a paper regarding the legal considerations when gathering online cyber threat intelligence and purchasing data from illicit sources (the "DoJ Paper").
The goal of the DoJ Paper is to inform private cybersecurity companies regarding the steps they should adopt in order to avoid violating US federal criminal law while conducting cybersecurity activity involving criminal forums, purchases of cryptocurrency, purchases in Dark Markets such as the TOR network, etc.
Here are some of the key points covered in the DoJ Paper:

• Collecting intelligence in a passive way usually is not illegal. However, gaining access to a forum in an unauthorized manner can implicate the US Computer Fraud and Abuse Act, and other statutes.
Information regarding an ongoing or impending computer crime that is uncovered during intelligence gathering activities should be promptly reported to law enforcement agencies.
• At the outset, federal prosecutors typically have not brought charges against parties who merely attempt to buy their own stolen data or to buy security vulnerability. However, a party engaged in those activities faces legal risks. There are some aspects that can have an impact in these cases, e.g. whether the purchaser is the legitimate owner of the data, the type of data and the seller's identity.
• Do not assume someone else's identity without that person's consent.
• When information is exchanged with cyber criminals, you should use systems that are not connected to the company network and that are properly secured.

• If your organization is gathering online cyber threat intelligence and purchasing data from an illicit source, or intends to do so, it should prepare a compliance program which contains guidelines in that regard.
• It is recommended to build an ongoing relationship with the local FBI field office or Cyber Task Force and the local US Secret Service Electronic Crimes Task Force.
• Seek legal advice with respect to issues arising on these issues.

Our compliance team usually advises clients on such matters and would be happy to assist as well as answer any question regarding the DoJ Paper.
For your convenience, please find attached the full version of the DoJ Paper here.

Contact Information

Yuval Z. Sasson, Partner
Cyber Security Groups
+972-3-6103190
ysasson@meitar.com

For additional information about our firm's Cyber Security group, click here.

This memorandum is provided solely for informational and educational purposes and should not be construed as a legal advice

---

To join our newsletter click here