(21)

Defendant's witness testimony (lead) [Garuda] For Court's Use

Black Case No. P3370/2566

Red Case No.

Civil Court

10 September B.E. 2567 (2024)

Civil Procedure

Between	Mr. Jatupat Boonpattararaksa	Plaintiff
	N.S.O. GROUP TECHNOLOGIES LTD.	Defendant

I, Witness, have sworn in and testify that:

1. I am Mr. Samuel Jacob Sunray *[TRANSLATOR NOTE: **VERBATIM**]*;
2. I was born on __ month __ B.E. __ Age 60;
3. My occupation is a company employee;
4. -
5. I am related to the Parties as the General counsel of the defendant.

And give further testimony that the Witness is an Israeli national and cannot testify in the Thai language. The Witness will testify in English with assistance from the interpreter, Ms. Urupan Suwannaprasop *[TRANSLATOR NOTE: **VERBATIM**]*, who has taken an oath.

Responding to The Defendant's Lawyer's Examination:

I testify that I certify this written transcript in place of today's witness examination.

Before I assumed the role of the Defendant's General counsel, I was a lawyer of 35 years. I was a former member of the Israeli Defense Force, serving in the International Legal Affairs Division at the entity called Military Advocate General. I have worked in international public law and international humanitarian law for over 30 years. I work with two major Israeli contractors. My work is worth billions of dollars. I am responsible for overseeing rules and regulations in over 70 countries and compliance with international regulations. I have experience with business law and domestic laws, including compliance.

In the early 2000s, surveillance of terrorists and criminals was conducted by eavesdropping. A judge will sign a warrant authorizing the police to eavesdrop through a Mobile Network Operator (MNO).

The world changed from 2007 to 2008 (B.E. 2550 - 2551). The first iPhone was introduced in 2007, and the first Android phone was introduced in 2008. It was good news for complying citizens who want to communicate with friends and families. It was even better news for terrorists and criminals because they could encrypt their communication and plans without the knowledge of the police and intelligence agencies.

Law enforcement and intelligence agencies became blind and deaf. There were no eyes or ears to foresee terrorist activities. There were international disagreements. Some governments believe that an effective countermeasure is mass surveillance, such as using a supercomputer or a computer capable of listening to all mobile devices in the country. Someone may come knocking on the door of those who utter on the phone to assassinate the president.

Some suggested using Backdoor Systems. If Apple, Google, or other mobile device retailers. A mechanism must be installed so the government can eavesdrop on the mobile device.

Both methods are undesirable, allowing governments to eavesdrop on every citizen's mobile device. This creates the need for tools like Pegasus, which are target-centric, meaning

they are directed toward one specific suspect. The judge could issue a target-specific warrant, in which time and data type may be specified. Such a method is more proportional and has more personal data protection.

As far as I know, Pegasus is the first tool that meets this objective.

While Pegasus was developed in 2010, the founders knew the tool had multiple benefits and risks. To quote Spider-Man, "Great power comes with great responsibility."

On the first day, the company decided to lay three ground rules for Pegasus.

Rule #1: The tool must be sold only to governments and government agencies. Many companies and individuals have proposed millions of dollars to the Defendant's company, but the company has declined to follow those requests.

Rule #2: The company will not sell [its products] to governments with which it is not confident they can meet proper objectives.

Rules #3: This tool must be handled according to regulations. The company alone cannot decide who to sell it to. The Israeli government must approve the sale and grant the receiving government software usage rights.

No regulations on the matters above were established in 2010. The company has a division that drafts regulations so that the government has a supporting regulation.

Pegasus Software allows the customer to use the software to determine targets on the end-user's data-encrypted device.

Pegasus's software arrives at the target's mobile device using infrastructure that starts from the customer's location and moves to the target's. The customer will transfer data through infrastructure to the device using a server, the means through which data sent from the customer could traverse and arrive at the target's device. There must also be a server that sends data from the target's mobile device back to the customer's location.

The Defendant created all of the infrastructure; however, the customer operates the system independently.

The Defendant cannot access any data or transfers in the computer system, whether it is data transferred from the customer's location to the end-user or from the end-user back to the customer's location.

This is an important matter for the Defendant, who is by no means related to the operation or the customer's data. The company's rules, which are compliant with its regulations and the Israeli government, prohibit such actions.

The Ministry of Defense of Israel hosts the Defense Export Agency (DECA), which operates under export control laws. These are criminal laws. DECA prohibits marketing, exporting, and transferring knowledge to end-users or foreign agencies without the agency's permission. As part of the permitting and licensing process, the Israeli government will examine records of human rights abuses by the end-user. It will not grant licenses unless the foreign government can produce a certification or pledge that said foreign government will use the software solely to prevent crime and terrorism.

This is a pledge between governments. There must be no abuse or violation of the pledge.

I have previously explained that the Defendant's company does not use, control, access, or have data on the government's actual use.

Items (28) and (30) of my Witness Testimony state, per my knowledge, that Plaintiff's claim in Document Jor.32 that the Defendant recorded or made copies of data on the Defendant's server is incorrect.

The Defendant's Lawyer asks about Activity log. *The Witness testifies that* it is part of the system that ensures that the customer has performed proper actions or recorded activities planted in the Software. The Log is at the customer's location and under the customer's control. The Defendant designed the software so the customer could not tamper with the Software system

or change Activity log. The Defendant cannot access that activity Log. The Defendant may use the Activity Log to investigate alleged misuse by requesting that the customer show the activity Log to the Defendant to prove that the system is used following proper objectives. I wish to reiterate that the Defendant cannot access the activity Log if the customer does not allow it.

Log Activity file is kept at the customer's location.

Item (30), the Blackbox Solution in paragraph 2, states that the Defendant provides a Blackbox Solution. According to the Defendant, a Blackbox means that the Defendant has no knowledge of the content, operation, or activities inside the box for which the Defendant holds no

key. Regarding Document Jor.33, I have explained in items (29) and (30) of my Witness Testimony. The Defendant's employees were not in the same room as the customer's office. The Defendant never received access to or requested the Blackbox.

The Defendant's Lawyer inquires whether the Defendant can access or assist customers remotely. [TRANSLATOR'S NOTE: From here, the testimony mixes third-person and first-person sentences in the same sentence and paragraph. For comparability purposes, I will italicize the dialogue parties. The subject of the following sentences should be regarded as the party in italics.]

The Witness replies as follows. As I have already testified, the Defendant had not accessed the customer's operating system, provided assistance to the customer, and did not offer any detailed supporting services. The Defendant offered the customer technical support and an upgrade for the software. Although the customer provided very limited access to Defendant to provide technical assistance, Defendant could not make any observation due to time and space constraints whenever permission was obtained.

The Witness further testifies about the customer's permission. Remote access is limited, and access is specific, as if time-constrained permission was given to pass through a small gate.

Remote access does not mean any action is allowed once accessed. All of the above means that Defendant provided less assistance than what normal software services would provide for their customers.

The Defendant's Lawyer asks why Pegasus software is not software-as-a-service. *The Witness replies that* Pegasus is not a service. Software-as-a-service (SAAS) provider method is when the provider provides cloud, a service the user may use from cloud. For example, Netflix maintains movies on a cloud. Customers can download movies once they become members. Pegasus is not a cloud service but software provided at the customer's location. Most importantly, Defendant had no service operation.

The Witness explains that "service" does not include an instance when the customer gives a number and requests data collection.

The Defendant's Lawyer asks what the Kill Switch Function means according to item (28) of the Witness Testimony. *The Witness testifies that* it is part of the program that operates according to the rules to enforce the customer's pledge. The company can sever the customer's connection with the system if an investigation finds that the customer has violated stated purposes or standard rules or does not cooperate with Defendant's investigation, such as denying Defendant's request to examine the activity log.

The Defendant's Lawyer shows the Witness Document Jor.55. *The Witness testifies* that he could not certify the correctness of this document.

The Defendant's Lawyer asks why The Defendant could not comply with the first request appended to the Plaint, which requests usage suspension. *The Witness testifies that* it is not possible to suspend an activity that has so far been unable to execute. The request was meaningless.

The Defendant's Lawyer asks why The Defendant could not comply with the second request appended to the Plaint, in which the Plaintiff asked for his data to be handed over. *The Witness testifies* that it is not possible to return something that is not in possession, like asking for the return of a diamond on the crown that is not there. The request was meaningless.

The Defendant's Lawyer asks if the Defendant was asked to testify about Documents Jor.34 and Jor.35. *The Witness testifies* that he had never been contacted by said organization.

The Defendant's Lawyer asks the Witness how he would testify to the National Human Rights Commission of Thailand. *The Witness says* he would testify to the Commission the same way he is testifying to the Court today and my Witness Testimony to the best of my abilities.

The Defendant's Lawyer asks the Witness how he would clarify the points raised in Document Jor.58. *The Witness says the following.* Firstly, we submitted answers to Amnesty International and published them yesterday per Document Lor.20, which the Defendant's Lawyer is showing me. I am surprised to see Document Jor.58. I believe Amnesty International is behind the thrust of this case. As far as I know, the Plaintiff's document is not submitted to this case. Crucially, the Defendant believes that he or she must reply to points raised in this letter. The article in Jor.58 criticizes the Defendant's human rights position, but the Defendant replies that he or she is proud of the company's position on this matter. The company has made pledges on global stages as well as Amnesty International. The company submitted a letter to Amnesty International but never received a reply.

I believe that there should be international consultation on rules.

I do not believe that Amnesty International's agenda protects human rights, and I believe that It is not in good faith. The Defendant's Lawyer asked the Witness why the customer names could not be disclosed. The Witness replied that the Defendant's customers are intelligence and law enforcement agencies, thus requiring serious considerations regarding protecting privacy and secrecy. Customers clearly expressed to the Defendant that the ways and means of intelligence data collection must be regarded top secret. If bad people, drug traffickers, pedophiles, or terrorists catch wind that an agency is using this tool, they may be able to evade. This point is important to the customers, and trust is vital in this relationship.

Responding to the Plaintiff's Lawyer's Cross-Examination

The Plaintiff's Lawyer asks if Document Lor.20 is distributed on the internet on the Defendant's website. *The Defendant* replies in the affirmative. *The Plaintiff's Lawyer asks* if it was

the first explanatory document that the Defendant used to explain to the public since Pegasus spyware was accused of violating personal rights. *The Witness states* that Pegasus is not a spyware but a software that legally collects information. This is not the first time we have received reports of wrongful use, and details will appear in the transparency report attached to the Witness Testimony and the previous transparency report. There is also a public statement from the company besides this one.

The Plaintiff's Lawyer asks if the Witness knew that per Document Jor.34, the National Human Rights Commission has no right to summon a private party to a deposition. *The Witness testifies* that he knew about neither the Human Rights Commission nor its regulations.

The Plaintiff's Lawyer asks at which point the Witness became aware of the facts in the Human Rights Commission report, as shown in Document Jor.34. *The Witness testifies that* he was aware of neither the report nor its findings.

The Plaintiff's Lawyer asks if the Defendant had ever produced a letter disputing the Commission or its findings. *The Witness testifies that* he knew nothing about the Human Rights Commission, its findings, or its report.

The Plaintiff's Lawyer asks if the Defendant, through the Defendant's Lawyer, had been invited to testify on the matter in which the Plaintiff's party filed a complaint. *The Witness states* that the Lawyer notified me that the Defendant accepted the invitation. *The Plaintiff's Lawyer asks* why the Witness did not testify. *The Witness testifies* that he had nothing besides what had been stated on this day.

The Plaintiff's Lawyer asks if the Witness served in the military while the specialist witness was testifying last week. *The Witness testifies that* he did not know.

The Plaintiff's Lawyer asks the Witness who was the person the Defendant knew and arranged for Mr. Yuval to become a witness. *The Witness testifies that* it was the General counsel.

The Plaintiff's Lawyer asks the Witness if he knew about the expenses associated with becoming a Defendant's specialist witness. *The Witness* declines to answer.

The Plaintiff's Lawyer asks the Witness if he bore the cost associated with becoming the Defendant's specialist witness. *The Witness answers that* the Defendant paid a fee and airfare to the testifying specialist.

The Plaintiff's Lawyer asks the Witness if he had personally communicated with the specialist witness before testifying. *The Witness answers that* he had met the specialist witness about a month prior but never previously. The Defendant's General counsel had never met the specialist witness. The recommendation of this specialist witness came from a cybersecurity expert. I explained to this specialist witness the overview of this case. This witness compiled an individual report. I contacted the specialist witness last week to have the person come to testify in Bangkok.

The Plaintiff's Lawyer asks the Witness whether or not the point at which the Defendant tries to have the specialist witness raise is only the fault in the Plaintiff's investigation. *The Witness answers that* he told the specialist to review the Plaint, the report, and the attachments to the Plaint, and consider what may support the Plaintiff's accusation. The specialist witness concluded that the said document could not prove the Plaintiff's accusation.

The Plaintiff's Lawyer asks if the Defendant has never disclosed the infrastructure, process, or methods of Pegasus Spyware to the specialist witness. *The Witness* replies in the affirmative but objects to the term Pegasus Spyware.

The Plaintiff's Lawyer asks the Witness to recount the organization of the Defendant's company. *The Witness replies* that the Defendant's company is like any other high-tech, companies, with employees, General counsels, and contains multiple teams such as Human Resources, Finance, Communications, Research and Development, Products, Sales, Customer Relations, and Legal and Compliance, the last of which I lead.

The Plaintiff's Lawyer asks whether the Witness is related to work in Research and Development, Sales, and Marketing. *The Witness replies that* he is not part of the teams mentioned but must work with Research and Development and Sales in management.

The Plaintiff's Lawyer asks if the Israel-registered Q Cyber Technologies Ltd. is a major shareholder in the Defendant's firm. *The Witness* replies in the affirmative.

The Plaintiff's Lawyer asks if Q Cyber Technologies develops software for penetrating systems similar to that of the Defendant's firm. *The Witness* replies in the negative. Firstly, the software does not penetrate a system. The is a clear division in the company organization. Within Q Cyber, Q Cyber is at the top, under which lies the Defendant's company who conducts research and development. The Defendant's firm owns intellectual property and intellectual property rights.

The Plaintiff's Lawyer asks if Q Cyber Technologies is the Defendant's firm's director and major shareholder. *The Witness replies* in the negative. There are two firms: Q Cyber and NSO Group Technologies. Q Cyber owns NSO, but each firm has its own function following organizational management principles. Each firm has authorized representatives and has a specific scope of work. *The Witness explains that* Q Cyber Technologies is the Defendant's firm's director and major shareholder.

The Plaintiff's Lawyer asks if Q Cyber Technologies is responsible for marketing of the Defendant's firm. *The Witness* replies in the affirmative.

The Plaintiff's Lawyer asks if Q Cyber Technologies markets Pegasus under the name Pegasus Software. *The Witness* replies in the affirmative.

The Plaintiff's Lawyer asks if the Defendant has another software similar to Pegasus called Minotaur. *The Witness* replies that he is not familiar with the word.

The Plaintiff's Lawyer asks if the Government of Israel is a major shareholder of Q Cyber Technologies. *The Witness* replies in the affirmative. *The Plaintiff's Lawyer asks* if Q Cyber Technologies is an Israeli government agency. *The Witness replies that* the Israeli government does not hold shares or own the company. The Defendant's company is private. The government is responsible for regulating, so it is unrelated to the government.

The Plaintiff's Lawyer asks if the sale of Pegasus in Israel is prohibited. *The Witness replies that* he will not link answers to questions about the Israeli government or any other governments, as previously answered.

The Plaintiff's Lawyer asks if Mr.[Chaim Gelfand] is also on the legal team besides the Witness. *The Witness* replies in the affirmative. He is the deputy division director, second to the Witness, and head of the Compliance division.

The Plaintiff's Lawyer asks if Mr. Chaim gave statements in the Defendant's place at the European Parliament in June 2022. *The Witness replies that* Mr. Chaim appeared at the European Parliament to explain the compliance and investigation processes similar to how the Witness is testifying to the Court today.

Afternoon Session (Witness continues testimony from the morning session.)

The Plaintiff's Lawyer asks if the European Parliament asked the Witness to clarify whether the Defendant's company produced or sold Pegasus Spyware without measures to prevent the spyware from being used against ordinary citizens. *The Witness testifies that* the Defendant has multiple measures to ensure that the tool is used correctly according to the appropriate objectives. These measures include vetting customers before the tool is sold and strict measures for responsibility and contracts stating what operations are permitted. There is a human rights seminar on what constitutes appropriate objectives and vice versa. In the event of inappropriate use, there will be a full investigation, technology control, supervision of authorization, geographic limitation, and more.

The Plaintiff's Lawyer asks if another point clarified to the European Parliament was whether the Defendant's company would shut the system down from further usage if a state experiences a seizure of power, coup d'état, or riot. *The Witness replies that* in if the power seizure presents human rights risks, then the system will be shut down.

The Plaintiff's Lawyer asks whether the shutdown is permanent or if the contract would be nullified. *The Witness testifies that a* kill switch would be used and the contract would be nullified.

The Plaintiff's Lawyer asks if the Defendant ever examined and found wrongful uses of Pegasus and, if so, how many contracts were canceled. *The Witness testifies that* there are 8 recorded cases.

The Plaintiff's Lawyer asks about those that are found not to have violated appropriate objectives or other's rights. *The Witness testifies that* there were multiple cases where the investigation found no wrongful use and there was no system shutdown.

The Plaintiff's Lawyer asks the Witness to explain the investigative process. *The Witness testifies that* there will be a technical examination of whether the customer is related to the Defendant's system. Then, the customer will be contacted. The Defendant's firm will ask for targeting data from the customer to examine whether targeting is legal and further request a warrant and its timeframe. Once all information is received, the Defendant's firm will verify the truth of that information and whether it covers human rights violations. The board of directors will convene and review all documents and evidence to decide how to proceed, which includes non-action, use of a kill switch, or system shutdown. Meanwhile, the customer may be cautioned, asked to change personnel or receive other requests depending on the result of the investigation.

The Plaintiff's Lawyer asks how will the Defendant's company know how the target the Witness mentioned is acquired. *The Witness says* the customer will be asked who the target is. If the customer admits, next steps will be taken. If the customer denies it, an audit or activity log will be requested to verify truthfulness.

The Plaintiff's Lawyer asks if it is a complaint or media report that prompts such investigation from the Defendant's firm. *The Witness says,* according to the report, the investigation starts from having all credible evidence, whether they are from media report, non-profit or non-government organization's report, or an informant. Our whistleblower policy accepts information from an internal and external source. If an employee hears anything from the customer and raises an issue, all of the above will trigger an investigative process. Nonetheles, what is raised must credibly point to a plausible operation resulting from using the Defendant's tool.

The Plaintiff's Lawyer asks if inappropriate uses were found in those 8 cases, and if there are any such uses in Southeast Asia. *The Witness replies that* he cannot answer because he cannot differentiate targets from customers.

The Plaintiff's Lawyer asks if inappropriate uses were found in those 8 cases, and if there are any such uses in Southeast Asia. *The Witness replies that* he cannot answer because he cannot differentiate targets from customers.

The Plaintiff's Lawyer asks if the Defendant's company is the sole producer, developer, and seller of Pegasus Spyware. *The Witness replies that* the Defendant's company is the sole producer and developer of Pegasus software.

The Plaintiff's Lawyer asks if the Defendant's website details properties and attributes of Pegasus Spyware. *The Witness replies that* the statement is inaccurate.

The Plaintiff's Lawyer asks if Pegasus Spyware aims to intrude the target's mobile device unbeknownst. *The Witness replies that* the Plaintiff's Lawyer uses terms that are inaccurate. Governments and law enforcement and intelligence agencies are users whose aim is to surveil terrorists and criminals. *The Plaintiff's Lawyer asks* if Pegasus Spyware is designed to intrude the target's mobile device unbeknownst. *The Witness replies that* Pegasus is not a spyware but Pegasus is used by government agencies.

The Plaintiff's Lawyer asks if a spyware program can intrude a target's mobile device unbeknownst. T*he Witness replies that* he has already answered the question. *The Witness replies* in the affirmative without using the term spyware, clarifying that it is used by government agencies.

The Plaintiff's Lawyer asks if Pegasus is designed to defeat protection. *The Witness replies* in the affirmative.

The Plaintiff's Lawyer asks if Pegasus is designed to defeat protection. *The Witness replies* in the affirmative.

The Plaintiff's Lawyer asks if it is true that, before 2020, Pegasus must send a link to the target, but since 2020, a link need not be sent, instead utilizing a Zero Click system. *The Witness testifies that* the statement is incorrect.

The Plaintiff's Lawyer asks if the Defendant develops the Zero Click system to complicate efforts to trace system intrusion. *The Witness testifies that* that is incorrect.

The Plaintiff's Lawyer asks if the Zero Click system is developed to protect from tracing to using customers. *The Witness testifies* in the affirmative. It is the primary tool to intrude a mobile device, whether through clicking a link or zero click. In both cases, the customer may choose which method to use. The criminals or terrorists should not know they are under surveillance the same way a person being eavesdropped must not be aware of the eavesdropping.

The Plaintiff's Lawyer asks if, n the production, development, and sales, there are risks that customers will use the product to violate personal rights. *The Witness testifies* in the affirmative. There are risks that the product will be used for inappropriate purposes. Therefore, the Defendant must control and prevent inappropriate uses, similar to a law enforcement officer cannot use firearms inappropriately when a gun is sold to the officer.

The Plaintiff's Lawyer asks whether the Defendant's company is free from responsibility if there are inappropriate uses of the product sold by the Defendant. *The Witness replies that* the Defendant is not responsible for inappropriate uses, but the Defendant has human rights obligations. Therefore, the Defendant will be responsible for specific cases that occur. If the inappropriate use occurs outside of control, the Defendant's company will not be legally responsiblea

The Plaintiff's Lawyer asks what human rights obligation does the Defendant has regarding the Witness' testimony on human rights. *The Witness replies that* the Defendant is obligated to operate according to the United Nations human rights principles, uphold and respect human rights. I hereby emphasize that it is like complying with any other laws such as anti-money laundering law and anti-foreign corruption law, which are legal obligations which the company must comply. However, the company is not legally liable to victims. For example, the bank is not

liable to victims of money laundering, but must strictly comply with the law or verify status. The bank must comply with rules if irregularities arise.

The Plaintiff's Lawyer asks whether or not the Defendant's company was blacklisted in the United States in November 2021 for selling products to a customer who subsequently use them to violate human rights. *The Witness replies that* the statement is incorrect.

The Plaintiff's Lawyer follows up by asking what measures did the U.S. government take. *The Witness replies that* the U.S. government used the Entities List to control technology exports from the United States to the Defendant. Export of controlled items must receive specific permission from the U.S. government. Similarly, the Israeli government controls military exports. The U.S. Department of State is responsible for military equipment export control, but there is also a list of export controlled items managed by the U.S. Department of Commerce. The Defendant's company is listed by the Department of Commerce. Previously free-flowing exports must now receive specific permissions. There is an appeal but a verdict has not been reached. *The Plaintiff's Lawyer asks* whether or not the Defendant's company remains on said list. *The Witness replies* in the affirmative.

The Plaintiff's Lawyer asks whether the allegation was that Pegasus Spyware was used to violate individual's rights. *The Witness reiterates* that Spyware is a misnomer *and that* the case was not about human rights, but that Pegasus software which the customer used violated Apple's ISO operating system in violation of computer laws.

The Plaintiff's Lawyer asks whether or not the Defendant's company was sued by WhatsApp in addition to Apple. *The Witness replies* in the affirmative. The case is pending trial. *The Plaintiff's Lawyer asks* if the Defendant's company is battling this case. *The Witness replies* that the Defendant's company has submitted a testimony. A pretrial examination of evidence is underway. The following steps are deposition and evidence gathering. Witness examination is not in the next step.

The Plaintiff's Lawyer shows document(s) to the Witness and asks if those documents are used in the WhatsApp case. *The Witness replies that* those documents are part of the appeal for dismissal and belong to a human rights professor. Many facts in the document are inaccurate.

Because the customer is a government entity, the customer could not be sued in the United States due to exclusive immunity. The document is an accusation, not related to the case pending trial.

The Plaintiff's Lawyer asks if the court orders the Defendant's company to hand over codes and passwords. *The Witness replies* that it is not entirely accurate. Per U.S. rules of evidence, there remains a dispute about the limit of evidence gather<<{add} "ing" {signature}>> between disputed parties. *The Witness replies that* some codes related to the case had been submitted.

The Plaintiff's Lawyer asks whether it is true that the Defendant has never denied or disputed the facts in Document Jor.52. *The Witness testifies* in the negative. The Document is part of the dispute over evidence gathering for a case in a U.S. court. Specifically, the dispute was over a specific file about the Amazon web server Service case, about evidence gathering between

disputed parties in a U.S. court. Document Jor.52 causes a misunderstanding. There remains a dispute between disputed parties over evidence gathering in the United States, concerning which party's subject may submit what evidence.

The Plaintiff's Lawyer asks if it is true that the Defendant's company adopted human rights as part of business policy because Pegasus Spyware was used to violate the rights of over 50,000 individuals. *The Witness replies* that it is not true. The policy was used long before the article was published. The article's statement about 50,000 targets is incorrect. There are 50,000 names because the customer created a list of phone number searches. The list is unrelated to the mobile device being infected with Pegasus or whether or not Pegasus was used in an operation. The article about 50,000 names is untrue. There is a newspaper article refuting the article in question.

The Plaintiff's Lawyer asks if the Witness knows the number of cases of inappropriate uses of Pegasus Spyware since the program was made. *The Witness replies that he* is not certain about the number of investigations, although many are concluded as false. There are 8 positive cases, and the connections were severed due to inappropriate uses. To estimate, there were about 100 investigations over the past 14 years since Pegasus was made. The number 100 is a

reasonable amount. As far as I know, the Defendant's company is the only one in the world that conducts investigations and shuts down systems.

The Plaintiff's Lawyer asks how the Defendant's company has been complying with human rights policy given that 35 political activists in today's case have been hacked by Pegasus, as published in the news globally. *The Witness replies that* although the assumption is that it was Pegasus, he disagrees. Our specialist witness has testified that it was not Pegasus. It is not possible to distinguish "customers" and "targets". I do not believe it is specifically related to the Defendant because it was the company's obligation. If the Defendant's product is believed to be used inappropriately, there will be a full investigation of the allegation, and appropriate measures will be taken.

The Plaintiff's Lawyer asks whether the fact that 35 political activists with similar aims were hacked nearly simultaneously is sufficient grounds for the Defendant to conduct an investigation. *The Witness replies that* he has already answered the question. If the evidence is credible, there will be an investigation. *The Witness emphasizes that* confirming or denying the specifics regarding customers or targets is impossible, but there will be an investigation into necessary matters.

The Plaintiff's Lawyer asks if the Defendant has not attempted to investigate whether the customer has in fact used Pegasus Spyware in manners that violate a contract and individual's rights with regards to the Plaintiff's case. *The Witness replies that* this is the same question, although worded differently, and he has already answered it.

The Plaintiff's Lawyer asks if the customer has clarified to the Defendant whether or not the customer has used Pegasus Spyware inappropriately. *The Witness replies that* this is the fifth time the same question was asked and worded differently.

The Plaintiff's Lawyer asks whether the Defendant has scopes or methods in purchasing in product sales negotiation for cases of rights violation due to the installation of a military government from a coup d'état. *The Witness replies that* this is a hypothetical question and never happened.

The Plaintiff's Lawyer asks whether it is true that the Defendant's company has never sold products to military or authoritarian governments. *The Witness replies that* he will not testify on this matter regarding customers.

The Plaintiff's Lawyer asks whether it is true that the sale of Defendant's company's products is conducted through private representatives in the customer's country. *The Witness replies* in the affirmative. There are two ways. First is direct sales to the government through a government contract. In some countries, it is sold through a reseller, such as in countries where value-added tax laws require a reseller to resell it. The reseller is an intermediary who helps achieve country-specific goals. The product's human rights obligation is a government-to-government matter. Customers must be under their obligations to sign, so it is an end-user matter. DECA, a government agency, will issue a certificate of approval for the end-user or their obligations, which the end-user or government must sign.

The Plaintiff's Lawyer shows Annex Korkai of Document Jor.24 to the Witness and asks whether the so-and-so brand and so-and-so series of Q Cyber's Minotaur belongs to Q Cyber, the parent company of the Defendant's company. *The Witness replies* that he does not know and will not certify the document as correct.

The Plaintiff's Lawyer asks whether only the parent company of the Defendant's company has the Q Cyber brand. *The Witness declines* to certify this document.

The Plaintiff's Lawyer asks whether it is true that the Defendant has never declined the facts as appeared in the news and this article per Documents Jor.30 and Jor.31. *The Witness replies* that he has testified according to his Witness Testimony on the morning of this day and has already testified regarding said documents. *The Plaintiff's Lawyer asks* whether the Defendant has ever declined the said documents prior to this litigation. *The Witness replies that* he does not know and testifies in this case according to the facts and the provided Witness Testimony.

The Plaintiff's Lawyer asks on what basis is the term lawful government used per item (11) of Witness Testimony. *The Witness replies* that he has explained about the verification process in the morning session and that the transparency report contains multiple verification steps. There

is an index scoring. It receives 9. A few factors are examined: records of the country's human rights examination, domestic media freedom index, a country's good governance, and the country's corruption level. Scoring is from 0 to 100. There is categorization. Risks, opportunities, and other factors are evaluated. Ways to analyze the likelihood of risk include a state or central government agency, E.U. export controls, U.S. export controls. Grades from A to D will be given as a country score. 64 is a B. Our due diligence process will evaluate whether the risk is low, medium, high, and if it is potentially on the rise.

The Plaintiff's Lawyer asks whether, should the necessity arise, the Defendant must receive a request to modify settings on the target characteristic limitation that the Defendant designed per item (15) of Witness Testimony only to suspected serious criminals and terrorists, and if the customer could modify such settings. *The Witness replies that* it is incorrect and the Defendant uses technical and contractual limitations.

The Plaintiff's Lawyer asks whether it is true that the customer could not modify the limitations to target characteristics. *The Witness replies that* it is not possible according to the contract.

The Plaintiff's Lawyer asks whether the program's system that determines the target group characteristics is located where the customer could not modify. *The Plaintiff's Lawyer rephrases and asks* whether these settings are in the program. *The Witness replies* in the affirmative.

The Plaintiff's Lawyer asks whether the Defendant will modify the settings for target characteristics according to the customer's request to add or set anew. *The Witness replies* in the affirmative. *The Plaintiff's Lawyer asks* whether the fact that the Defendant will modify settings according to the customer's request demonstrates that the Defendant knows who the new target group is and whether the group may not be criminal. *The Witness replies* in the negative.

The Plaintiff's Lawyer asks whether the fact that the Defendant executes the customer's request to modify settings demonstrates that the Defendant knows of the risk that the program may be used against the new target group and that human rights may be abused. *The Witness replies* in the negative. If the customer requests a change in authorization quantity, such as from the original quantity in the contract of 10 to 12, the Defendant will verify whether the request is

appropriate and grant additional rights accordingly. The Plaintiff's Lawyer's question is not related directly, to target collection, or to the knowledge of the target.

The Plaintiff's Lawyer asks whether the Defendant knows who the target is from the initial targeting. *The Witness replies in the negative*. If the target group is unknown, the individual is unknown.

The Plaintiff's Lawyer asks whether the Defendant could access the system security section without permission, to which the customer is denied access. *The Witness replies in the negative*.

The Plaintiff's Lawyer asks whether an examination would yield traces of the program, according to item (19) of Witness Testimony on attack tracing of Pegasus and other spyware programs per Documents Lor.2 through Lor.5. *The Witness replies in the negative*.

The Plaintiff's Lawyer asks if it is the case that the Witness does not know that the software program in item (19) is used to hack the Plaintiff in this case, and that the Witness has no information. *The Witness replies in the affirmative*. I do not know if Pegasus or another program was used in the attack on the Plaintiff.

The Plaintiff's Lawyer asks how the operating system of Pegasus spyware and spyware in item (19) differ. *The Witness replies that* he does not know.

Responding to the Defendant's Lawyer's Re-direct Examination

No further questions/reading.