

INTERNATIONAL COURT OF JUSTICE

THE REPUBLIC OF INDIGO (APPLICANT)

v.

THE FRANK REPUBLIC (RESPONDENT)

2019

INTERNATIONAL COURT OF JUSTICE

SPECIAL AGREEMENT

BETWEEN REPUBLIC OF INDIGO (APPLICANT)

AND FRANK REPUBLIC (RESPONDENTS)

TO SUBMIT TO THE INTERNATIONAL COURT OF JUSTICE

THE DIFFERENCES BETWEEN THE STATES CONCERNING TWIGGLE

Jointly notified to the Court on 30 January, 2019

JOINT NOTIFICATION

ADDRESSED TO THE REGISTRAR OF THE COURT:

The Hague, January 30, 2019

On behalf of Applicant, the Republic of Indigo, and Respondent, the Frank Republic, and in accordance with Article 40(1) of the Statute of the International Court of Justice, we have the honor to transmit to you an original of the Special Agreement for submission to the International Court of Justice of the Differences between the Applicant and the Respondent concerning Twiggie, signed in The Hague, The Netherlands, on the thirteenth day of January in the year two thousand nineteen.

(Signed)

For Republic of Indigo

Minister of Foreign Affairs

(Signed)

For Frank Republic

Minister of Foreign Affairs

SPECIAL AGREEMENT

SUBMITTED TO THE INTERNATIONAL COURT OF JUSTICE BY THE REPUBLIC OF INDIGO AND FRANK REPUBLIC ON THE DIFFERENCES BETWEEN THEM CONCERNING TWIGGLE

The Republic of Indigo (“Applicant”) and the Frank Republic (“Respondent”) (hereinafter “the Parties”);

Considering that differences have arisen between them concerning Twiggle and other matters;

Recognizing that the Parties have been unable to settle these differences by direct negotiations; Desiring further to define the issues to be submitted to the International Court of Justice (“the Court”) for resolution;

In furtherance thereof the Parties have concluded this Special Agreement:

Article 1

The Parties submit the questions contained in the Special Agreement (together with Corrections and Clarifications to follow) (“the Case”) to the Court pursuant to Article 40(1) of the Court’s Statute.

Article 2

It is agreed by the Parties that the Republic of Indigo shall appear as Applicant and the Frank Republic as Respondent, but such agreement is without prejudice to any question of the burden of proof.

Article 3

The Court is requested to adjudicate the claims of the Republic of Indigo specified in paragraphs 22-23 below, applying the rules and principles of international law, including any applicable treaties, in accordance with Article 38, paragraph 1, of the Statute of the Court.

Article 4

- (a) Procedures shall be regulated in accordance with the applicable provisions of the Official Rules of the International Moot Court Competition of SVKMS’NMIMS University, Kirit P. Mehta School of Law.
- (b) The Parties request the Court to order that the written proceedings should consist of Memorials presented by each of the Parties not later than the date set forth in the Official Schedule.

Article 5

- (a) The Parties shall accept any Judgment of the Court as final and binding upon them and shall execute it in its entirety and in good faith.
- (b) Immediately after the transmission of any Judgment, the Parties shall enter into negotiations on the modalities for its execution.
- (c) In witness whereof, the undersigned, being duly authorized, have signed the present Special Agreement and have affixed thereto their respective seals of office.

(Signed)

For Republic of Indigo
Minister of Foreign Affairs

(Signed)

For Frank Republic
Minister of Foreign Affairs

AGREED STATEMENT OF FACTS

1. The Republic of Indigo (“Indigo”) and the Frank Republic (“Frank”) are sovereign nations, permanent members of the Security Council, United Nations and members of the World Trade Organization. Indigo and Frank are also signatories to the *Treaty on Privacy and Data Protection between Indigo and Frank* (attached in “Annexure A”) entered into following discussions on the need to ensure protection of privacy of citizens on the internet.
2. The Republic of Indigo is a land-locked developing nation and former British colony, with one of the largest populations in the world. Its economy has so far been mostly agricultural, but Indigo has experienced rapid economic growth in the last decade.
3. Frank Republic is a developed nation and is a member of the Kinder Union (“KU”). The KU has developed an internal single market through a standardized system of laws that apply in all member states. Frank’s rapidly-expanding information technology and communications sector is world-renowned.
4. The Government of Frank has played a major role in the growth of Frank’s information technology sector. The Government’s Department of Technology has invested millions of dollars in the industry. Till 2012, the government held 71% stake in Frank’s largest social media company, Twiggle Corporation (“Twiggle”) headquartered in Papertown, Frank, which was established in 2008. In September 2012, Twiggle started providing cloud storage services to its users. Following concerns of user privacy and government access to large amounts of user data from the international community, the Government of Frank adopted a legislation to privatize the Twiggle in November 2012. Shares of Twiggle have been publicly traded on Frank’s largest stock exchange since 2013 and currently, the Frank government holds 12% shares.
5. Twiggle went global in 2010, and is now the largest social media and cloud storage company in the world with users from all continents. Twiggle has campaigned vigorously to expand its user base in all developing countries with attempts to tie – up with major telecom companies in developing countries to provide access to Twiggle for free. As per reports from 2017, Indigo has the largest user base in Twiggle with users using both its social media as well as cloud features.

6. Twiggle's cloud service has been made available as an ancillary to their social media services, where Users can store, for free – their pictures, videos, as well as archives of their previous conversations. The Terms of Use in “Annexure B” are applicable to their cloud storage platform as well.
7. In an attempt to grow its customer base, Twiggle has spent several hundred million dollars to make its services accessible to all sections of the public. Twiggle today has an easily accessible interface with a simple sign-up process. When a person creates an account on Twiggle (User), they are required to provide their name, address, contact numbers and e-mail address. Once these details are given, Users (who are only natural persons) are directed to a page containing the Terms of Use of Twiggle (attached in Annexure B).
8. On September 26 2018, there was an outage on Twiggle servers, where multiple users of the social media platform, as well as those who store their data on the Twiggle cloud not access their profiles or their data. Twiggle released a statement on September 27, 2018 stating that it was a minor technological malfunction and the servers would be up and running as soon as possible.
9. On October 5, 2018, a known terrorist group Lasha-o-Maida announced that they had hacked into Twiggle servers and had gained access to the personal data of 24 million users. The terrorist group is known for using social media as a tool to recruit members and to communicate with members in different nations.
10. The announcement caused public out roar around the world. Several governments launched investigations against Twiggle to determine if the data breach was a threat to their nation. As part of these investigations, it was revealed that Twiggle had been selling user data to several third parties including companies engaged in big data, data profiling, marketing and advertising agencies. One such company is Valentino Corporation which compiles user data and provides this information to Twiggle and other companies for targeted advertisements. In response to this, Twiggle released a statement on November 16, 2018 stating that Twiggle obtained consent from all its users for transfer of data to third parties for advertising and enhancing user experiences.
11. On November 20, 2018, world known data privacy expert Ms. Ivy Leaks published a piece on a leading newspaper's website arguing that Twiggle's consent provisions were vague and inadequate. Ms. Leaks argued that Twiggle's use of user data by Twiggle and companies to which data had been transferred went beyond advertising and was an invasion of privacy. Ms.

Leaks further argued that such use was not limited to enhancing user experiences, but was purely for Twiggle's illicit commercial gain.

12. The Government of Indigo took note of this development, as Lasha-o-Maida is believed to have carried out several bombings within its territory. In 2009, Lasha-o-Maida took responsibility for a shooting of Mahal Taj, a famous hotel in the city of Tombay in Indigo. The Indigo Government is worried that with the kind of data that Lasha-o-Maida has in their control, Lasha-o-Maida will have the ability not only to track Indigo citizens with Twiggle profiles, but also have the ability to carry out attacks.
13. On December 12, 2018, Twiggle released a statement that its internal investigations had revealed that the data breach had been caused by two Users – Manila Luzon and Sasha Velour who own and manage a public page under the name Indigo-Nation on Twiggle where they post geo-tagged photographs of high ranking officials of the Indigo government and Indigo army. Manila Luzon and Sasha Velour are believed to be aliases used by two citizens of Indigo who have links to Lasha-o-Maida.
14. Following Twiggle's announcement, the Indigo Law Enforcement Agency controlled by the Ministry of Security of Indigo wrote to Twiggle on December 15, 2018 seeking all information on the users Manila Luzon and Sasha Velour. The contents of the letter have been attached as "Annexure C" with this Compromis.
15. On December 17, 2018 Twiggle made the letter public and refused to provide the data sought by the Indigo Government citing privacy concerns. Twiggle's CEO, Ms. Alyssa Edwards released the following statement:
"While we confirm receipt of this letter from the Mr. Bonobo of the Indigo Law Enforcement Agency, we must respectfully deny access to the requested information. Twiggle is a company incorporated in the Republic of Frank, and hence we are obligated to provide User information only to the Government of Frank, should we receive such a request. We believe that releasing the requested data to the Indigo Government will result in not only a breach of privacy of our Users, but would also lead us to go against our Terms of Use. We however confirm that should the Government of Frank request us to provide such information, we will release the specified information to them."
16. When asked about the Indigo Government's move, Ms. Leaks commented that acceding to the Government requests would result in gross invasion of privacy by Twiggle. Ms. Leaks was firmly of the belief that should the requested data be released, not only the suspected terrorists

data would get shared, but the data of those individuals who had even an indirect association with such content would be released as well.

17. On December 20, 2018, an attempt to assassinate Mr. Cotton Park, the top-most military official in Indigo was carried out in Tombay, Indigo. Following the attempt, news reports linked the attacks to Lasha-o-Maida and published posts made on Indigo-nation with details of Mr. Cotton Park visiting his daughter in Tombay. Members of the opposition party in Indigo made accusations that the Government of Indigo did not take enough action to curb the activities of Lasha-o-Maida. This inaction further enraged the citizens of Indigo who felt agitated at the failure of their long-standing government to protect them.
18. In response to accusations, the Indigo government arrested four men in relation to the data breach and possible attacks on officials of the Indigo government. The detainees were kept in a detention center in a small town near Tombay. On December 25, 2018, the Indigo Government released a press statement stating that the men detained belonged to Lasha-o-Maida. This information was confirmed through narco analysis conducted for the purpose of obtaining information about further attacks planned by Lasha-o-Maida. News reports suggest that the men detained are citizens of Frank.
19. Mr. Camo Namu, a data privacy expert known to be affiliated with the Indigo government appeared on primetime news and stated:
“Twiggle’s acts are in gross violation of their duty to protect the privacy of individuals and to act in accordance with their Terms of Use, upon with Users register with their site. Their indiscriminate sale of User data, along with their inability to protect their data from the likes of Lasha-o-Maida has led to a series of terrorist activities. In particular, their actions are in violation of their treaty obligations of data minimization, consent, third party transfers, and security measures, for starters.”
20. On December 30, 2018, Mr. Bonobo Takir, Chief Inspector, of the Indigo Law Enforcement Agency sent a letter to the Frank Government requesting them to take steps for the release of the requested data. The Frank Government later released a statement that Frank’s legal provisions do not permit them to access/request access to Twiggle’s servers, and they were under no obligation to release this data to Indigo. The statement also mentioned that the Indigo Government themselves had acted in violation of international law by conducting narco analysis tests.

21. Officials from Home Ministries of both Frank and Indigo met at a Summit on January 26, 2018 and decided to submit their dispute to the International Court of Justice for adjudication. On January 30, 2018 the representatives signed a Special Agreement conferring jurisdiction upon the International Court of Justice to hear and settle this dispute.

22. The Republic of Indigo respectfully requests the Court to hold that:

- Frank is responsible for the acts of Twiggie in violation of the Treaty because Twiggie's actions are attributable to Frank.
- Twiggie's consent provisions violated the Treaty's provisions;
- Government of Indigo can obtain data of its citizens from Twiggie to ensure national security and peace within its sovereign territory;
- Declare that the narco analysis test conducted by Indigo is not in violation of international law

23. The Frank Republic respectfully requests that the Court reject each of Applicant's claims in its entirety, and specifically requests the Court to hold that:

- a. The acts of Twiggie are not attributable to the Frank Government
- b. There has been no violation of treaty
- c. There has been no violation of the right to privacy
- d. Declare that the use of narco analysis test conducted by Indigo amounts to torture and is violation of international law

Parties are free to add/amend/seek deletion the prayers at the International Court of Justice. The hearing as been fixed for 15th – 17th March 2019.

ANNEXURE A

Treaty on Privacy and Data Protection between Indigo and Frank

WHEREAS

The Contracting Parties recognise that:

- *Every individual has a right to life, liberty and security of person, as envisaged under Art. 3 of the Universal Declaration of Human Rights;*
- *Although national laws and policies may differ, Contracting Parties have a common interest in protecting privacy and individual liberties and in reconciling fundamental but competing values such as privacy and the free flow of information.*

Article 1

Subject-matter and objectives

1. This Treaty lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Treaty protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. Contracting Parties shall give effect to the provisions of this Treaty. Contracting Parties may, but shall not be obliged to, implement in their law more extensive protection than is required by this Agreement, provided that such protection does not contravene the provisions of this Agreement. Contracting Parties shall be free to determine the appropriate method of implementing the provisions of this Agreement within their own legal system and practice.

[...]

Article 3

Territorial scope

1. This Treaty applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the territory of a Contracting Party, regardless of whether the processing takes place in the Contracting Party or not.
2. This Treaty applies to the processing of personal data of data subjects who are in the in the territory of a Contracting Party by a controller or processor not established in the territory of a Contracting Party, where the processing activities are related to:

- (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the territory of a Contracting Party; or
 - (b) the monitoring of their behaviour as far as their behaviour takes place within the territory of a Contracting Party.
3. This Treaty applies to the processing of personal data by a controller not established in the territory of a Contracting Party, but in a place where a Contracting Party's law applies by virtue of public international law.

[...]

Article 5

Principles relating to processing of personal data

1. Personal data shall be:
- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
 - (d)
 - (e)
 - (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
 - (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

[...]

Article 17

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
- (c)
- (d) the personal data have been unlawfully processed;
- (e)
- (f)

[...]

Article 27

1. Any dispute between the Contracting Parties concerning the interpretation or application of Articles of the present Treaty shall be submitted at the request of either Contracting Party to the International Court of Justice.

ANNEXURE B

Excerpts from the Terms of Use of Twiggle

- e. *“Personal Information” - Information that we collect depends on your use of Twiggle Products, i.e. our social media and cloud storage platforms (“Products”). Since our Products are provided to you free of cost, you accept that we may use your data for specified purposes. Things that you and others do and provide:*
- ***Information and content you provide.*** *We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content and message or communicate with others. This can include information in or about the content that you provide (e.g. metadata), such as the location of a photo or the date a file was created. Our systems automatically process content and communications that you and others provide to analyse context and what's in them for the purposes described below.*
 - ***Networks and connections.*** *We collect information about the people, pages, accounts, hashtags and groups that you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups that you are part of.*
 - ***Your usage.*** *We collect information about how you use our Products, such as the types of content that you view or engage with, the features you use, the actions you take, the people or accounts you interact with and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products.*
 - ***Information about transactions made on our Products.*** *If you use our Products for purchases or other financial transactions (such as when you make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information, other account and authentication information, and billing, delivery and contact details.*
 - ***Things others do and information that they provide about you.*** *We also receive and analyse content, communications and information that other people provide when they use our Products. This can include information about you, such as when others share or comment on a photo of you, send a message to you or upload, sync or import your contact information.*
- f. *By providing us your information, you hereby consent to the collection, storage, disclosure, processing and transfer of such information for the purposes as disclosed in this Policy and directly/indirectly consented to by you. You are providing the information out of your free will. You have the option not to provide us the data or Personal Information sought to be collected if you do not agree with this Policy.*
- g. *Purposes – we may use your Personal Information for purposes including but not limited to the enhancement of User services, targeted advertisements, marketing and advertising purposes*
- h. *You authorize us to transfer your Personal Information with our affiliates / agents / third party service providers / partners and for purposes as consented to by you or as may be required by law.*

- i. *The security of your Personal Information is important to us. We have adopted reasonable security practices and procedures.*

ANNEXURE C

Letter written to Twiggle by the Indigo Law Enforcement Agency

To,

Ms. Alyssa Edwards,

Chief Executive Officer,

Twiggle Inc.

Dear Ma'am,

Subject: Invasion of Privacy of Indigo Users of Twiggle

I write to you in unfortunate circumstances where certain developments have led us to doubt not only Twiggle's security measures but also Twiggle's policies of sharing of User data. While we may discuss these issues at length in the coming months, we have a more pressing concern on our hands. On December 12, 2018, Twiggle released a statement that your internal investigations revealed that the data breach of September 2018 had been caused by two Users, namely Manila Luzon and Sasha Velour – which appear to be aliases used by the notorious terrorist group Lasha-o-Maida.

While the hacking of Twiggle by Lasha-o-Maida remains of great concern to us as the privacy of Indigo citizens is at risk, we have received confirmation that the Twiggle page 'Indigo-nation' is run by the very same Manila Luzon and Sasha Velour, where they post photographs and the verified locations of high ranking officials of the Indigo government and Indigo army. We see this as not only a severe security breach, but also a threat to the safety of such officials.

For this reason, we request that you give us access to Twiggle servers in order for us to access any and all information and data relating to the profiles and activity of Manila Luzon, Sasha Velour, 'Indigo-nation' and any other data that we should find relevant to have ties back to Lasha-o-Maida. This access includes (but is not limited to) their social media profiles, access to the profiles of those who follow/like/comment on their posts and pages, any communication sent from their profiles, and access to relevant cloud storage accounts as we may request.

We hope that you appreciate the gravity of the situation and co-operate as soon as is reasonably practical.

Many thanks,

Bonobo Takir,

Chief Inspector,

Indigo Law Enforcement Agency