

**IN THE SUPREME COURT OF VICTORIA
AT MELBOURNE
COMMON LAW DIVISION
MAJOR TORTS LIST**

No. S ECI 2019 01926

BETWEEN

NICOS ANDRIANAKIS

Plaintiff

-and-

UBER TECHNOLOGIES INCORPORATED
and other according to the attached schedule

Defendants

GENERAL FORM OF ORDER

JUDICIAL OFFICER: The Honourable Justice Macaulay
DATE MADE: 21 December 2020
ORIGINATING PROCESS: Writ filed on 3 May 2019
HOW OBTAINED: Pursuant to directions made 4 November 2020
ATTENDANCE: On the papers

THE COURT ORDERS THAT:

Discovery Plan

- 1 The Defendants provide discovery to the Plaintiff of:
 - (a) documents of which the Defendants are, after a reasonable search, aware at the time that discovery is given and which:
 - (i) unless otherwise specified, fall within the Discovery Period, as defined in **Annexure 1**; and
 - (ii) are responsive to the categories in **Annexure 1**;
 - (b) further, documents which meet at least one of the criteria specified in rule 29.01.1(3) of the *Supreme Court (General Civil Procedure) Rules 2015* (Vic) and which the employees of the Defendants who provide instructions to the solicitors with carriage of this proceeding (including external



solicitors and inhouse legal counsel) or the solicitors with carriage of this proceeding are aware without making searches.

- (c) For the purpose of satisfying their obligation to make reasonable searches for documents responsive to the general categories in **Annexure 1**, the Defendants will apply a Technology Assisted Review process in accordance with the Technology Assisted Review Protocol at **Annexure 2**.

- 2 Discovery is to be given by the defendants in three tranches, namely, the first tranche to be provided by 4:00pm on 29 January 2021, the second tranche to be provided by 4:00pm on 15 March 2021 and the third tranche on a date to be determined at the directions hearing referred to at paragraph 6 below.
- 3 The Plaintiff is to provide discovery to the Defendants pursuant to Order 29.01.1 of the Rules by **4:00pm on 23 December 2020**.

Electronic Document Exchange Protocol

- 4 The parties shall comply with the Electronic Document Exchange Protocol at **Annexure 3** to this order.

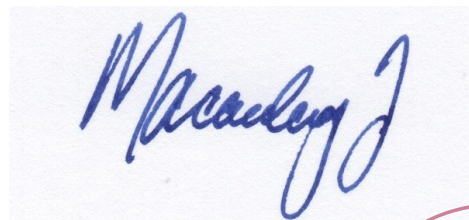
Security for Costs

- 5 The defendants file and serve any application for further security for costs, together with any supporting affidavit and outline of submissions, by **4:00pm on 29 January 2021**.

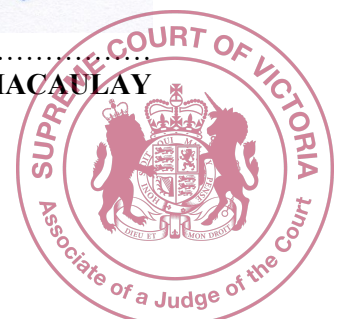
Timetable

- 6 The matter be listed for directions on **26 March 2021 at 10:00am**.
- 7 Liberty to apply.
- 8 Costs are reserved.

Dated: 21 December 2020.



.....
THE HONOURABLE JUSTICE MACAULAY



SCHEDULE OF PARTIES

NICOS ANDRIANAKIS

Plaintiff

- and -

UBER TECHNOLOGIES INCORPORATED (4849283)

First Defendant

UBER INTERNATIONAL HOLDING B.V. (RSIN 851 929 357)

Second Defendant

UBER B.V. (RSIN 852 071 589)

Third Defendant

UBER AUSTRALIA PTY LTD (ACN 160 299 865)

Fourth Defendant

RASIER OPERATIONS B.V. (RSIN 853 682 318)

Fifth Defendant

UBER PACIFIC HOLDINGS B.V. (RSIN 855 779 330)

Sixth Defendant

UBER PACIFIC HOLDINGS PTY LTD (ACN 609 590 463)

Seventh Defendant



Discovery categories

Notes:

Terms defined in the Further Amended Statement of Claim and Consolidated Amended Defence have the same meaning when used in these categories.

Discovery Period means the period from 1 January 2012 to 23 August 2017.

General categories

1.	All high level documents that record: <ol style="list-style-type: none"> lines of reporting; business objectives; allocation of functions and responsibilities; and governance, <p>as between the Uber Entities in respect of the Uber Business.</p>
2.	All documents that record reports to Uber Inc about the Uber Business in Australia.
3.	Documents forecasting or recording UberX's market share in the Australian point to point passenger transport market.
4.	Any documents that record, refer or relate to the numbers of individuals or vehicles in the Australian States who or which met or may have met the Compliance Requirements.
5.	All documents that record, refer or relate to: <ol style="list-style-type: none"> the strategy for establishment and operation of the Uber Group in various countries or markets outside of the United States of America to the extent they record or evidence a strategy to build scale prior to the legalisation of ridesharing in those countries or markets; the strategy for establishment and operation of the Uber Business in Australia; the launch of the Uber Business in Australia, (including in any of the Australian States) including any strategy relating to the launch; the launch of the UberX Product in Australia, (including in any of the Australian States) including any strategy relating to the launch(es).
6.	All documents that discuss or record plans or strategies for the uptake, expansion or promotion of UberX in Australia (including in any of the Australian States) including <ol style="list-style-type: none"> any incentives for existing or potential UberX Partners and Riders; and the development and implementation of any marketing campaigns for the Uber app and Uber Partner app.
7.	Documents that refer or relate to competition between UberX and other Point to Point Passenger Transport Services (howsoever described), including: <ol style="list-style-type: none"> any competitive advantage obtained by the UberX Partners and/or the Uber Entities who did not satisfy the Compliance Requirements; and any upfront or ongoing costs or other savings or advantages experienced by UberX Partners and/or the Uber Entities if they did not comply with any



	of the Compliance Requirements and/or the requirements set out in Schedule 2 to the Defences.
8.	Documents (including budgets and staff reports) that discuss, refer or relate to regulatory authorities and government representatives in connection with the launch or operation of the UberX Product in the Australian States, including: <ul style="list-style-type: none"> a. engagement in connection with the launch or operation of UberX; b. strategies for dealing with any risks and costs associated with regulatory action or potential regulatory action in relation to Uber X; c. securing a favourable regulatory environment for the operation of UberX, including but not limited to low barriers to entry for UberX or UberX Partners and regulatory change that would have the effect of legalising or rendering lawful the operation of UberX; d. strategies, policies, practices or procedures in respect of enforcement action against UberX Partners by a regulator in relation to UberX; e. regulators or law enforcement bodies in each of the Australian States either expressly or tacitly not enforcing the relevant regulations or bringing any enforcement action against any of the Uber Entities.
9.	Documents that refer or relate to: <ul style="list-style-type: none"> a. The Compliance Requirements for point to point transport in the Australian States. b. The lawfulness, unlawfulness and/or potential unlawfulness of the UberX Product (including UberX Driver Partners or potential UberX Driver Partners) in the Australian States, including without limitation any legal advice or discussion or consideration of any legal advice.
10.	Documents (including budgets and staffing reports) that evidence, record or refer to the development, implementation and discontinuance of Greyball in the manner alleged in paragraph 67 of the FASOC (whether directly or indirectly) in the Australian States, including: <ul style="list-style-type: none"> a. policies for its deployment; b. technical design documentation; c. tagging of accounts for application of Greyball; and d. data demonstrating the application of Greyball or any tagging of Riders or trips associated with such software.
11.	All documents that record or discuss: <ul style="list-style-type: none"> a. recruitment of Uber Partners; b. recruitment of Uber Riders; and c. support services for UberX Partners or potential UberX Partners, including but not limited to vehicle inspections and the renting of premises, in Australia.
12.	All documents that record, refer or relate to the drafting and publication of the Uber Policy White Paper 1.0, including any drafts.
13.	All documents that record, refer or relate to communication(s) with Uber Partners or Riders about the regulatory environment for the operation of UberX.
14.	All documents that record: <ul style="list-style-type: none"> a. setting the minimum vehicle standards; b. the entity responsible for the minimum vehicle standards; c. communications to UberX Partners and potential UberX partners about the minimum vehicle standards; d. compliance and enforcement of the minimum vehicle standards



	in respect of vehicles used to provide UberX in the Australian States.
15.	All documents that discuss, refer to or relate to the requirements for UberX Partners to comply with contractual terms imposed by any of the Uber Entities on UberX Partners, including but not limited to: <ul style="list-style-type: none"> a. any consideration of compliance in the drafting of terms; b. any step taken by or on behalf of any of the Uber Entities to enforce or ensure compliance with these terms; and c. any consideration of an intention, or any decision or direction, to enforce or not enforce these terms.
16.	All documents discussing, recording or referring to fines, infringement notices or penalty notices issued to UberX Partners in the course of providing UberX in any of the Australian States, including but not limited to: <ul style="list-style-type: none"> a. records of the fines, infringement notices or penalty notices; b. documents relating to payment (directly or indirectly) of the fines, infringement notices or penalty notices, including but not limited to any reimbursement of UberX Partners; c. documents relating to procurement of payment of the fines, infringement notices or penalty notices; d. charges laid or prosecutions of UberX Partners; e. communications with UberX Partners concerning such fines, infringement notices or penalty notices or any charges laid or prosecutions, or any consideration or discussion concerning such communications.
17.	All documents recording or referring to the terms 'network liquidity', 'building scale' or 'network effect/s' prior to the legalisation of ridesharing in countries or markets outside the United States of America



Specific categories

18.	Financial statements of each of the Uber Entities.
19.	Policies or documents evidencing financial and or signing authority conferred to general managers (howsoever called) for the Australian States.
20.	Documents recording the registered partnership between the sixth and seventh Defendants.
21.	Licence(s) which govern the licensing of software in the Uber app and Uber Partner app in the Australian States including any related agreements.
22.	A representative sample of the documents or agreements, including each material iteration, which record or govern the relationship between any of the Uber Entities and Uber Driver Partners in the Australian States, including – <ul style="list-style-type: none"> a. the registration, creation and activation of personal accounts; b. contractual terms; c. service fees (however called); d. procedures for receiving information received from third parties about prospective UberX Partners.
23.	A representative sample of the documents or agreements, including each material iteration, which record, or govern the relationship between any of the Uber Entities and Riders in the Australian States, including the registration, creation or activation of personal accounts.
24.	A representative sample of any documents which governed the supply of Smartphones to UberX Driver Partners in the Australian States.
25.	All standard communications from any of the Uber Entities to UberX Driver Partners or Riders in the Australian States.
26.	Records of the following UberX trip data in the Relevant Locations and time periods set out in Schedule 1 to the Amended Defence: <ul style="list-style-type: none"> a. Date; b. Start/end time; c. Base fare; d. Confirmation that the base fare was paid by the Rider; e. Longitude and Latitude co-ordinates of start and end point; f. City; g. Trip mileage; h. Duration of trip; i. Suburb or post code of Riders’ pick up and drop off locations j. Licence or vehicle plate number of the UberX Partner k. The Application or surge pricing or other levies or surcharges, however, so described; l. Unique Rider Identification; m. Unique Driver Identification; n. The application of Greyball or any tagging or otherwise of Riders or trips associated with such software, for the purpose alleged in paragraph 67 of the FASOC.
27.	Corporate travel records for travel to and/or from Australia from 2012 to 2017 for Travis Kalanick, Austin Geidt, Ryan Graves, David Plouffe, Jordan Condo, Salle Yoo, Joe Sullivan and Nick Gicinto.



28.	Documents which evidence the following: a. Uber Inc providing financial support to Uber Australia in the period 2012 to 2013. b. Uber Holdings guaranteeing ongoing financial support to Uber Australia in the period October 2012 to the end of the Discovery Period.
29.	All documents that record the Playbook or Playbooks in respect of city/country launches, evading crackdowns, use of Greyball, VTOS or any like subject matter.
30.	Any Board minutes or papers between 2010 and 2018 for the Uber Entities which are responsive to the general categories.
31.	All final organisational charts (howsoever called) in which two or more of the Uber Entities appear.
32.	A list of all Riders who held accounts that were subject to the use of Greyball in the Australian States as alleged in paragraph 93 of the Statement of Claim.
33.	Any published or final versions of documents comprising advertising, marketing or promotions of UberX to prospective UberX Partners and Riders in Australia.



Technology Assisted Review Protocol





PROPOSED TECHNOLOGY ASSISTED REVIEW PROTOCOL

Nicos Andrianakis

and

Uber Technologies Incorporated and Others

Taxi Apps Pty Ltd

and

Uber Technologies Incorporated and Others

Dated: 5 November 2020

1. TAR Tool

1.1. The Defendants will employ H5 Technology-Assisted Review (**TAR Tool**).

2. Corpus

2.1. The Defendants will apply the TAR Tool to a corpus of documents comprising the mailboxes, Google Drive and the hard drives of the custodians who held a Relevant Position listed in Schedule 1 (**TAR Corpus**).

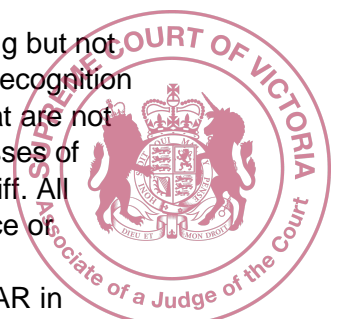
2.2. For the purpose of Clause 2.1, only the hard drives of the following custodians will be included in the TAR Corpus:

2.2.1. former employees of the Defendants; and

2.2.2. current employees of the Defendants who hold potentially relevant documents on their hard drives.

2.3. All documents that consist of images of primarily text files (including but not limited to image-only PDFs) will be subjected to optical character recognition and the extracted text loaded into the TAR Tool. All documents that are not suitable for TAR will be identified. The Defendants will identify classes of documents that are not suitable for TAR, and report them to Plaintiff. All documents in these classes will be manually reviewed for relevance or another method as agreed by the parties.

2.4. The TAR Corpus minus documents identified as not suitable for TAR in

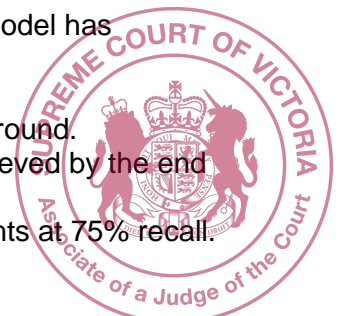


accordance with Clause 2.3 (**TAR Population**) will be processed in accordance with Sections 3 through 8.

2.5. The Defendants will report to the Plaintiff the size of the TAR Population.

3. Training

- 3.1. The TAR Tool will assign a number representing the probability of relevance (**Probability of Relevance Score**) to each unreviewed document.
- 3.2. The Defendants will identify an initial set of 'training' documents (**Seed Set**) which it will manually review and label for relevance (**Manual Review**). The persons who conduct the Manual Review of the Seed Set must be Australian lawyers of Associate level or higher (**Defendants Seed Set Reviewers**).
- 3.3. The Defendants will create the Seed Set by drawing a simple random sample of 500 documents (families to be reviewed at the same time) from the TAR Population.
- 3.4. The Defendants Seed Set Reviewers will perform a Manual Review of all documents in the Seed Set to:
 - 3.4.1. label them for relevance in accordance with Clause 3.2; and
 - 3.4.2. Identify documents for which the Defendants makes a claim of privilege. The identification of any documents by the Defendants as privileged in the Seed Set does not in any way affect the entitlement of the Plaintiff to challenge any claims for privilege.
- 3.5. The Defendants will draw a simple random sample of at least 1,000 documents from that part of the TAR Population that is still unreviewed (**Confirmation Sample**), and Manually Review those documents for relevance. The persons who conduct the Manual Review of the Confirmation Sample must be Australian lawyers of Associate level or higher. The sample will not be drawn until the corpus has been fully ingested into the TAR Tool.
- 3.6. The Defendants will report to the Plaintiff the proportion of the Confirmation Sample that is labelled relevant (**Confirmation Richness**).
- 3.7. Following the Seed Set review, the Defendants will perform iterative training of the model. The Defendants will employ the Active Learning mechanism of the TAR Tool to select training documents for labelling during iterative training (**Active Learning**). The persons with supervision of document review as part of the iterative training of the model must be Australian lawyers of Associate level or higher.
- 3.8. The Defendants may also employ alternative methods for identifying training documents, including but not limited to keyword and metadata searches, random sampling, or corpus browsing.
- 3.9. Iterative training of the model will continue until the Defendants determine that the model has achieved at least 75% recall and 40% precision (**Model Stabilisation**). Model Stabilisation will be determined against the Confirmation Sample.
- 3.10. When the Defendants contend that Model Stabilisation has occurred, the Defendants will report the following information to the Plaintiff:
 - 3.10.1. The total number of training documents labelled;
 - 3.10.2. The number of training documents labelled relevant;
 - 3.10.3. The basis upon which the Defendants claim that the model has stabilised;
 - 3.10.4. For the final training round:
 - 3.10.4.1. The number of documents labelled in that round.
 - 3.10.4.2. The estimated precision at 75% recall achieved by the end of that training round.
 - 3.10.4.3. The projected number of relevant documents at 75% recall.



4. Validation Sample

- 4.1. When Model Stabilisation has occurred, the Defendants will first draw a simple random sample of 500 records from the portion of the TAR Population identified as relevant by the TAR Tool as the **Precision Sample**.
- 4.2. The Defendants will label the Precision Sample for relevance. The Precision Sample will be labelled by no more than 2 reviewers (**Defendants Validation Reviewers**). The Defendants Validation Reviewers must be Australian lawyers of Associate level or higher.
- 4.3. Upon completion of the Precision Sample, the Defendants will draw a simple random sample (**Validation Sample**) from that part of the TAR Population that is still unreviewed (including any documents subject to bulk coding) (**Review Target Set**). The Validation Sample will be reviewed by the Defendants Validation Reviewers. The size of the sample will be determined by the results of the Precision Sample review, the size of the Review Target Set and sized sufficient to achieve a 95% confidence \pm 5% margin of error estimate of recall. The Validation Sample will not be sized less than 500 records or greater than 2,000 records.
 - 4.3.1. Should a 2,000 record Validation Sample be used and will not meet the 5% margin of error target, the Defendants will provide notification to Plaintiff what the resulting margin of error will be.
- 4.4. Upon completion of the review of the Precision and Validation Samples the Defendants will calculate and provide resulting summary statistics for recall and precision, including the associated margins of error for each statistic and report these results to Plaintiff.
- 4.5. The Defendants will produce any documents found in the validation process to be relevant. These documents will be clearly marked to indicate that they originated from the validation process. If any unique, relevant documents are identified in the course of the validation process, the parties will meet and confer about next steps, including further training or application of the TAR Tool as required.
- 4.6. Should the resulting statistics from the Precision and Validation Samples not meet the minimum threshold of 75% recall and 40% precision, the Defendants will conduct additional training of the TAR model in order to meet this threshold with sufficient precision as measured against the Confirmation Set.
- 4.7. Upon re-stabilisation after any steps taken pursuant to 4.5 or 4.6, the Validation process will restart with new samples selected.
 - 4.7.1. Any documents used during initial validation efforts will remain eligible for re-sampling so long as they are not used for TAR training, but any existing validation labelling will be removed to ensure a blind review during validation.

5. Cut-off Selection

- 5.1. The Defendants will use the Predictive Model to assign a Probability of Relevance Score to each document in the Review Target Set.
- 5.2. The Defendants will select the Probability of Relevance Score cut-off that the TAR Tool estimates will achieve at least 75% recall based on the Validation Sample. Documents in the Review Target Set with a Probability of Relevance Score at or above this cut-off will form the set of documents to be reviewed (**Review Set**).
 - 5.2.1. The Defendants will report to the Plaintiff:
 - 5.2.2. The number of documents in the Review Target Set but outside the Review Set (Unreviewed Set);
 - 5.2.3. The estimated number of relevant documents in the Review Set, based upon the Precision Sample; and
 - 5.2.4. The estimated number of relevant documents in the Unreviewed Set, based upon the Validation Sample.



6. Review of the Review Set

- 6.1. As relevant documents that are not subject to a claim of privilege (**Non-Privileged Relevant Reviewed Document**) are located by the Defendants, they will be produced to the Plaintiff in tranches, in accordance with the protocol for the electronic exchange of discoverable documents as agreed between the parties. Family members of each Non-Privileged Relevant Reviewed Document will also be produced, unless they are subject to a claim of privilege. The schedule for the production in tranches will be agreed with the Plaintiff at the outset of the Review of the Review Set.
- 6.2. All documents that are subject to a claim of privilege will be manually reviewed.

7. Quality Control Checks

- 7.1. The Defendants will utilise email threading, hash duplicate identification, text duplicate identification, and any other analytic tools determined to be reasonable and effective to perform initial quality control against documents labelled as irrelevant in order to correct manual labelling errors prior to taking any other remediation steps.

8. Other Matters

- 8.1. If the Defendants form the opinion during processing that any conditions of this protocol will not be able to be met, or would be disproportionately burdensome to meet; or if the Defendants form the opinion that the TAR Tool is unable to achieve satisfactory accuracy on the TAR Population; the Defendants will promptly notify the Plaintiff, state the reasons for its opinion, and confer with the Plaintiff on appropriate measures to take in response. Disputes on these appropriate response measures will be resolved by a Registrar of the Court or as the Court determines.
- 8.2. The Defendants may use any additional methods at their discretion to identify likely relevant material for review, including but not limited to alternative predictive models, keyword search, or browsing of key custodial email threads or file drive folders.
- 8.3. If the Defendants form the opinion that any document selection method other than those described in this protocol is likely to identify a high proportion of relevant documents, they will include documents selected by this method in the Review Set.
- 8.4. If the Defendants code any documents the subject of the TAR Protocol based on relevance without manual review, for instance, by bulk coding of document types or based on other metadata, details of the bulk coding undertaken will be provided to the Plaintiff. Disputes will be resolved by a Registrar of the Court or as the Court determines.
- 8.5. All documents discovered by the Defendants pursuant to this protocol shall be provided to the Plaintiff in accordance with the terms of the protocol for the electronic exchange of discoverable documents as agreed between the parties.



Schedule 1

Relevant Positions

1. Regional General Manager
 2. Head of Public Policy, APAC
 3. General Manager, ANZ
 4. Head of Public Policy and Government Relations, ANZ
 5. Head of Communications, ANZ
 6. General Manager, NSW/Sydney
 7. General Manager, VIC/City Lead Melbourne
 8. General Manager/ Head of State, QLD
 9. General Manager, WA/ City Lead, Perth
 10. Manager, Public Policy and Government Relations
 11. Operations and Logistics Manager, Sydney
 12. Operations and Logistics Manager, Melbourne
 13. Operations and Logistics Manager, Brisbane
 14. Operations and Logistics Manager, Perth
 15. Marketing Manager, Sydney
 16. Marketing Manager, Melbourne
 17. Marketing Manager, Brisbane
 18. Marketing Manager, Perth
 19. Senior Associate, Public Policy and Government Relations
 20. Expansion Manager
 21. Head of APAC Legal
 22. Head of ANZ Legal
-



Relevant Positions

23.CEO, Uber Technologies Incorporated (**UTI**)

24.Vice President Operations / Senior Vice President of Global Operations, UTI

25.Senior Vice President / Vice President of Policy and Communications, UTI

26.Head of Global Public Policy, UTI

27.Head of Global Expansion, UTI

28.Head of Asia Expansion

29.Launcher, Australia/ Senior International Launcher, Australia

30.Chief Legal Officer

31.General Counsel



Electronic Document Exchange Protocol



**Maurice
Blackburn**
Lawyers

Since 1919

**PROTOCOL FOR THE ELECTRONIC EXCHANGE OF DISCOVERABLE
DOCUMENTS**

Nicos Andrianakis

and

Uber Technologies Incorporated and Others

Version dated: 2 September 2020

Table of Amendments to Protocol

LEGAL ADVISER NAME	DATE OF AMENDMENT



Index to Protocol

1.	Introduction	3
2.	Electronic Exchange of Documents	4
3.	Document Numbering System	5
4.	Imaging of documents	6
5.	Discovered material which will not be imaged	6
6.	Hard Copy Document Processing Methodology	7
7.	Redaction of Privileged Hard Copy Documents	8
8.	Electronically Sourced Documents Processing Methodology	10
9.	Redaction of Privileged Electronically Sourced Documents	12
10.	Exchange of Court Documents	13
11.	Exchange of Subpoenaed Documents/Notice to Produce Documents ...	13
12.	Exchange of Large Volume Data types	14
13.	Quality Assurance	15
14.	Privilege Clawback	15
15.	Virus Responsibility	16
16.	Responsibility for Costs	16
17.	Updating or Adding Additional Data	16
	SCHEDULE 1	17
	PROPOSED PARTY CODES	17
	SCHEDULE 2	18
	HARDCOPY DOCUMENT FIELDS	18
	SCHEDULE 3	24
	ELECTRONICALLY SOURCED DOCUMENT FIELDS	24
	SCHEDULE 4	30
	LIST OF HARDCOPY DOCUMENT TYPES	30



1. Introduction

1.1 The parties to this Protocol are:

Nicos Andrianakis

Plaintiff

Uber Technologies Incorporated

Uber International Holdings B.V.

Uber B.V

Uber Australia Pty Ltd

Rasier Operations B.V.

Uber Pacific Holdings B.V.

Uber Pacific Holdings Pty Ltd

Defendants

This Protocol has been prepared for the electronic exchange of discoverable documents and electronic court documents between the Parties. It is designed to minimise the document management and technology costs and to ensure that the Parties are in agreement as to the format of the electronic exchange. It has been prepared in accordance with the Practice Note SC Gen 5 – Technology in Civil Litigation.

1.2 This Protocol has been prepared to enable:

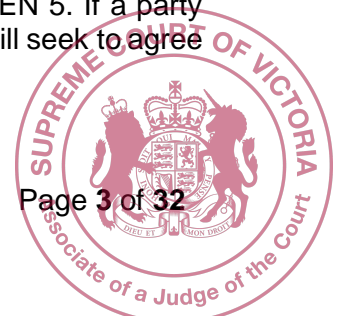
1.2.1 hard copy documents to be imaged and objectively coded; and

1.2.2 electronically sourced information, that is, Emails, Email Attachments and electronic files (“Efiles” as set out in clause 8.8, 8.9 and 8.10), to be processed in order to allow appropriate metadata to be captured for each electronic document and be converted to an appropriate image format.

1.3 Each party intends to use their own litigation support system to view data and images that have been prepared and exchanged in accordance with this Protocol.

1.4 Each party, if requested and entitled, will have the right to inspect the original discovered documents, where such originals exist.

1.5 Each party will utilise the best technology and practices in preparation of discovery, including, if considered appropriate, the use of technology assisted review (TAR), as indicated at 8.7 to 8.9 of Practice Note SC GEN 5. If a party proposes to utilise TAR in preparation of discovery, the parties will seek to agree on a protocol on the use of TAR.

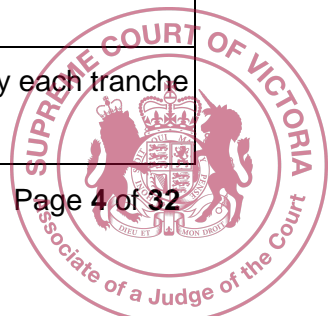


2. Electronic Exchange of Documents

2.1 The documents will be exchanged in accordance with this section.

2.2 Data and images will be provided as follows:

ITEM	PROTOCOL
Data Format	<p>Indexed data will be exchanged in an Access MDB file named export.mdb in a four table structure:</p> <ul style="list-style-type: none">• Export table – contains core field information for each document;• Export_Extras table – contains additional fields to the core fields;• Parties table – contains people & organisation information for each document;• Pages table – contains file name information for images that make up each document.
Image Format	OCR PDF in the directory structure outlined in clause 4.5
Native Document Format	<p>1) Files listed in clause 8.10 will be provided in native format.</p> <p>2) Native files will be renamed according to its Document ID and the relevant file extension.</p> <p>3) The original native file name will be captured as a metadata field as set out in Schedule 3, clause 20.4 “File_Name”.</p>
Extracted Text Format	Text file containing the text extracted from the native file, excepting where a document has redactions
Exchange Medium	<p>Appropriately sized USB (universal serial bus) stick or secure FTP (File transfer protocol) directly between the parties to enable the exchange of discoverable data.</p> <p>Guidelines - for a data set where transfer takes longer than 1 hour, a USB is preferred</p>
Contents	One file named export.mdb and all image and native files in the directory structure set out in clause 4.5.
Covering Letter	A covering letter will accompany each tranche of discovery



3. Document Numbering System

- 3.1 Each page of each document should be uniquely stamped with a number that accords with the document numbering system described in this section. The first page of each document will be stamped with a unique document id and the follow pages will be uniquely stamped by page ID.
- 3.2 Unless agreed otherwise, the document numbering system has four levels and every Document ID must appear as follows, **AAA.BBB.FFF.DDDD**, where:
- 3.2.1 **AAA** is the "Party" code, which identifies the party that has produced the documents. Proposed Party Codes are set out in Schedule 1.
 - 3.2.2 **BBB** is a three digit sequential box number. For hard copy documents, every box of documents held by a party will be allocated a box number. For electronic documents, the box number is a "virtual" box number. Padded zeros will be used when the box number is less than 3 digits.
 - 3.2.3 **FFF** is a three digit sequential folder number. Each folder within each box held by a party will be allocated a folder number. For electronic documents, "virtual" folder numbers may be created within each "virtual" box. Padded zeros will be used when the folder number is less than 3 digits.
 - 3.2.4 **DDDD** is a four digit sequential document number, which will increase by one for each new document. Padded zeros will be used when the page number is less than 4 digits.
 - 3.2.5 **_SSSS** is a four digit sequential number used for page 2 onwards within a document. Page 1 of the document uses the format outlined in 3.2.1 to 3.2.4 whilst from page 2 onwards, the '_SSSS' format is added as a suffix to each document number. Padded zeros will be used when the page number is less than 4 digits.

For example, using the methodology outlined above, the first two documents within the first folder of box 1 will be:

Document 1 – a 4 page document

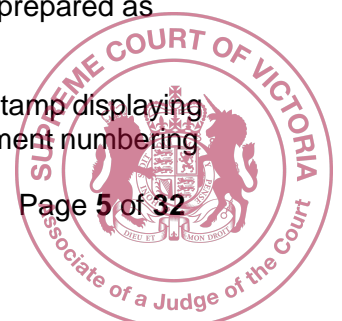
AAA.001.001.0001
AAA.001.001.0001_0002
AAA.001.001.0001_0003
AAA.001.001.0001_0004

Document 2 – a 3 page document

AAA.001.001.0002
AAA.001.001.0002_0002
AAA.001.001.0002_0003

- 3.3 Every page in a document will be allocated a page number and prepared as follows:

- 3.3.1 Every page will be numbered with a label or electronic stamp displaying the relevant Document ID in accordance with the document numbering



system discussed at clause 3.2 above.

3.3.2 All documents rendered to PDF, hard copy and electronic, will be electronically stamped with a number.

3.3.3 The stamp will appear as near as practicable to the top right of each page, according to the orientation of the majority of the text on said page. The stamp should not cover any text.

4. Imaging of documents

4.1 For hard copy and electronic documents, all images should be exchanged as multi-page PDF files with OCR for full text searching or in their native format.

4.2 All documents will also be accompanied by a text file (.txt), containing the extracted text for the corresponding native file, except where the document contains redactions, in which case a text file will be extracted from the redacted PDF of that document

4.3 Images should be black and white (except where colour is essential in order to make sense of the original document) and of a resolution of 300dpi (except where a higher resolution is necessary in order to make sense of the document).

4.4 PDF, native files, and text files will be named in accordance with the full Document ID for e.g. AAA.001.001.0001.pdf.

4.5 The image files are to be stored in directories that are divided into sub-directories reflecting the number of levels in the numbering convention: party\box\folder\.

4.6 Documents which are completely blank must not be imaged. Parties will make efforts to exclude non-relevant system files (eg Thumbs.db) and attachments (eg email signature gifs) from the discovered material.

5. Discovered material which will not be imaged

5.1 Material which may not be readily imaged (“**non-imaged items**”) will be treated in accordance with this section and includes the following:

5.1.1 Physically bulky items which cannot be imaged e.g. models;

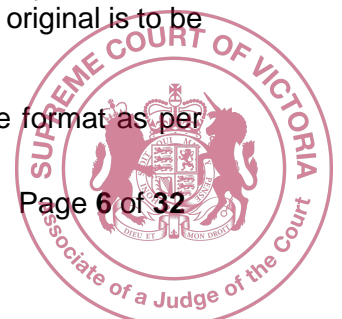
5.1.2 Material that is held in analogue formats e.g. videotape.

5.2 Non-imaged items will be listed within the discovery lists and the exchanged data, and will be represented by a numbered page inserted into the database describing the items.

5.3 The original items are to be made available for inspection to the Parties upon request by a party.

5.4 Documents up to A0 in size should be scanned at the original size. Any documents larger than A0 should have the bottom right corner only scanned to A4, ensuring that the title box is displayed on the image, and the original is to be made available for inspection upon request by a party.

5.5 Databases will be not be imaged and will be provided in native format as per clause 8.10.



5.6 Automatically generated system files, such as Thumbs.db, are not to be imaged or exchanged, where this is not possible, the parties are to code such documents to the export extras field **Non relevant system file** as per clause 20.4.

5.7 Parties will make efforts to avoid having embedded email signature images treated as attachments. If this is not possible, the parties are to code such documents to the export extras value **Non relevant system file** as per clause 20.4

6. Hard Copy Document Processing Methodology

6.1 Documents sourced in hard copy will be processed differently to those documents sourced in electronic format. Hard copy documents will be processed in accordance with this section.

6.2 Fields to be captured - The objective fields to be captured with respect to documents sourced in hard copy are set out in the table structure in Schedule 2.

6.3 Delimiting - The first page of each document will be delimited. Documents will be delimited objectively by using information and context derived from the face of the document. If there is any doubt as to whether a group of consecutive pages forms one document or several individual documents, the pages will be delimited as individual documents.

6.3.1 All documents will be delimited as Host/Attachment or Unattached.

6.3.1.1 A **host** document must be immediately followed with one or more attachment documents.

6.3.1.2 An **attached** document can only follow a host document.

6.3.1.3 An **unattached** document cannot be followed by an attached document.

6.3.1.4 A document will only be delimited as a host document if it can be ascertained from the face of the document that one or more of the documents immediately following it is an attachment to it. The source document must contain the words “enclosed”, “attached”, “following” or derivatives thereof. For example, please find enclosed, please find attached, enclosed herewith ... etc.

6.3.2 Where there are multiple documents on one page, the page will be delimited as one document.

6.3.3 If the pages of a document are not in order, but it is clearly identifiable as one document, it will be delimited as such.

6.3.4 Dividers will be delimited if there is information on either side of them. Blank dividers will not be delimited.

6.3.5 The backs of pages with text or markings will not be delimited as separate documents.



- 6.3.6 Annexures, attachments and schedules which form part of:
- 6.3.6.1 An agreement, will not be delimited as separate documents, but will be considered part of the agreement;
 - 6.3.6.2 A report, financial report or annual report, will not be delimited as separate documents, but will be considered part of the report;
 - 6.3.6.3 Legal documents, including affidavits, witness statements, pleadings etc will not be delimited as separate documents, but will be considered part of the legal document;
 - 6.3.6.4 The minutes of meetings or meeting agendas, will not be delimited as separate documents, but will be collectively considered as part of the meeting minutes or agenda.

6.4 Post-it Notes and document tags

- 6.4.1 All blank Post-it notes and document tags removed from the document for processing should be returned to the documents.
- 6.4.2 Where a Post-it Note exists and it has text written on it, the following is to be undertaken
- 6.4.2.1 Where it obscures text:
 - (a) The page is to be scanned as is to show the page with the Post-it exactly as it appears; and
 - (b) The Post-it is then to be removed and the page scanned without the Post-it note.
 - (c) The Post-it note is then to be scanned and numbered as the next page.
 - (d) Upon completion, the page is to be reinstated exactly as first found with the Post-it note replaced in its original position.
 - 6.4.2.2 Where it does not obscure text:
 - (a) The page is to be scanned as is to show the page with the Post-it exactly as it appears.
 - (b) Post-It Notes will not be numbered separately.
 - (c) The Post-it Note is to remain in situ; the page is to be scanned “as is” to show the page with the Post-it Note as it appears.

7. Redaction of Privileged or Sensitive Customer Hard Copy Documents

- 7.1 If the whole or part of a document:
- 7.1.1 is subject to a claim of privilege; or
 - 7.1.2 contains information that is

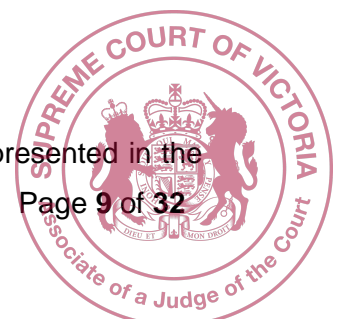


- (i) wholly irrelevant to the issues in dispute; and
- (ii) constitute a customer name, phone number, street address (excluding suburb and state) or credit card number

(sensitive customer information)

the parts of the document that are subject to the claim should be identified and, if appropriate, redacted or de-identified pending determination of the claim. If the whole or part of the document is redacted or de-identified, the party producing the document must retain an un-redacted or identified version of the document which must be produced to the Court if required to do so.

- 7.2 If the Court makes an order, or the parties subsequently agree, that the whole or part of a document is not subject to privilege, or does not contain sensitive customer information, the producing party must re-provide a version of the document which is either un-redacted or identified, or redacted or de-identified only to the extent permitted or agreed (**Un-redacted Version**). This un-redacted version must be assigned the same Document ID as the original, with a suffix “_U”, indicating it is un-redacted, and produced in accordance with this protocol.
- 7.3 If the whole or part of a Document is subject to a claim of privilege or contains sensitive customer information it will be:
- 7.3.1 allocated a Document ID;
 - 7.3.2 given a Document Description that does not disclose the information that is the subject of the claim of privilege or the sensitive customer information; and
 - 7.3.3 if the document:
 - 7.3.3.1 is wholly subject to a claim of privilege – represented by a single Placeholder Page with the words ‘Document subject to claim of privilege’ inserted under the Document ID; or
 - 7.3.3.2 wholly contains sensitive customer information – represented by a single Placeholder Page with the words ‘Document contains sensitive customer information’ inserted under the Document ID.
- 7.4 If the whole or part of a Host Document is subject to a claim of privilege or contains sensitive customer information it will be:
- 7.4.1 identified as a Host Document;
 - 7.4.2 allocated a document ID;
 - 7.4.3 given a document description that does not disclose the information that is the subject of the claim of privilege or the sensitive customer information; and
 - 7.4.4 if the document:
 - 7.4.4.1 is wholly subject to a claim of privilege represented in the



- Document Group to which it belongs by a single Placeholder Page with the words 'Document subject to claim of privilege' inserted under the Document ID; or
- 7.4.4.2 wholly contains sensitive customer information – represented in the Document Group to which it belongs by a single Placeholder Page with the words 'Document contains sensitive customer information' inserted under the Document ID.
- 7.5 If the whole or part of an Attached Document is subject to a claim of privilege or contains sensitive customer information it will be:
- 7.5.1 identified as an Attached Document;
- 7.5.2 allocated a Document ID;
- 7.5.3 given a Document Description that does not disclose the information that is the subject of the claim of privilege or the sensitive customer information; and
- 7.5.4 if the
- 7.5.4.1 is wholly subject to a claim of privilege relates – represented in the Document Group to which it belongs by a single Placeholder Page with the words 'Document subject to claim of privilege' inserted under the Document ID; or
- 7.5.4.2 wholly contains sensitive customer information – represented in the Document Group to which it belongs by a single Placeholder Page with the words 'Document contains sensitive customer information' inserted under the Document ID.

8. Electronically Sourced Documents Processing Methodology

- 8.1 Discoverable documents may be in electronic form.
- 8.2 In order to ensure cost efficiencies and to retain full metadata, documents that are electronic in their original form will not be converted to hard copy prior to processing. Electronic documents will be processed in accordance with this section.
- 8.3 All Efiles should be rendered to PDF with full text searching. Those file types that do not lend themselves to conversion to PDF (for example, Excel spreadsheets) will be exchanged in their native format. Those file types that are to be exchanged in native format are listed in 8.10.
- 8.4 The text from the native eFile will also be extracted and captured in a separate text file (.txt), which will be provided along with the PDF/native. If redactions are required, this text file will contain extracted text from the rendered, redacted PDF.
- 8.5 Any speaker notes, annotations, mark-ups, tracked changes and hidden text contained within an Efile will be captured when rendered to PDF. Any native files listed under clause 8.9 that are rendered to PDF without capturing these will be made available in their native format upon request (see clause 8.10).

8.6 Electronic data and documents may comprise one of the following formats:

8.6.1 Emails;

8.6.2 Email Attachments;

8.6.3 Efiles.

8.7 The objective fields and metadata to be collected for Emails, Email Attachments and Efiles is set out at Schedule 3.

8.8 The following file types will be treated as "Email" files. Email files will be exchanged as text-searchable PDFs:

MSG .msg files
EML .eml files
DBX MS Outlook Express files
Other email file types (including Lotus Notes, Groupwise etc).

8.9 The types of Efiles to be processed in accordance with this section and provided in text-searchable PDF format includes (but is not limited to):

DOC Microsoft Word Document
PPT Microsoft Office PowerPoint
JPG Joint Experts Group Format Files (JPG File)
GIF Graphical Interface Format (GIF File)
PDF Adobe Portable Document Format (PDF File)
TIF Tagged Image Format Files (TIFF File)
TXT Text file
RFT Rich Text Format
HTM HyperText Markup

8.10 Electronic documents listed below are Efiles and will be retained in their native format, unless otherwise agreed between the Parties. The following electronic documents are to be retained in their native format:

XLS Microsoft Excel Spreadsheet
MDB Microsoft Access Database
CAD CAD Drawings
MP3, WAV, Audio and Video files
MPEG etc
XML, CSV, Chat/Instant Messenger Records
JSON

Other file extensions that are agreed upon by the Parties and individual files pursuant to clause 8.5.

For the avoidance of doubt, if an electronic document is produced in native format the producing party will not need to produce a PDF placeholder image dating that the file has been produced in native format.

8.11 De-Duplication of Electronic Documents

8.11.1 The MD5 cryptographic hash value (MD5 value or similar unique



technical value) assigned to stand alone Efiles will be used to identify potential duplicate documents.

- 8.11.1.1 All stand alone Efiles will be de-duplicated against other standalone Efiles only.
- 8.11.2 Email Attachments will not be compared to Efiles that are not Email Attachments, to ensure the integrity of the Host and Attachment relationship.
- 8.11.3 Any Efile that is not an Email Attachment will be a duplicate of any other Efile that is not an Email Attachment that has the same MD5 value.
- 8.11.4 Only one 'master' document will be produced, and duplicates will not be produced.
- 8.11.5 All emails will be de-duplicated against other emails generating a hash value from the email metadata.
- 8.11.6 An example of a generated hash for email deduplication is as follows: where the time and date sent, the sender, the recipient(s), the CCs and the subject are identical. If the Email has Email Attachments, the number of Email Attachments and the MD5 value for each Email Attachment must be identical.
- 8.11.7 The parties will keep a log detailing all instances of documents which are not produced pursuant to this section.

8.12 Embedded files

- 8.12.1 Embedded files will be extracted from each Efile and exchanged as separate documents.
- 8.12.2 Where the embedded file is contained within another Efile, the file from which the embedded file was extracted will be the host and the embedded file/s will be the attachment/s.
- 8.12.3 Where an Efile with an embedded file is attached to an Email, the Email will be the host, the original file will be an attachment to the Email and the embedded file will also be an attachment to the Email.
- 8.12.4 The full file path for each file after it is extracted will be captured and exchanged.
- 8.12.5 When processing email embedded image files should not be extracted as separate attachments but rather should be imaged as part of the email.

Often blank attachments or logo image files will be unintentionally extracted by processing software as attachments. If a reasonable method is used to identify these files they may be withheld from the discovery and the host email should be coded as "Erroneous Extraction Issue" = Yes.

8.13 Password Protected files

- 8.13.1 Where an Efile is password protected, parties will undertake reasonable efforts to provide the Efile without such password



protection.

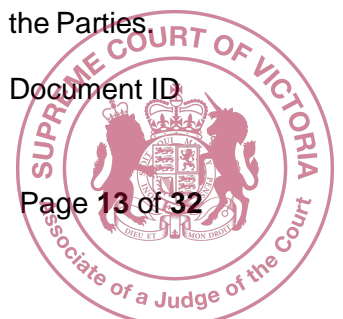
- 8.13.2 If the password is unable to be removed after reasonable efforts, the native file will be provided along with a PDF placeholder and the Password_Protected field in the "Export_Extras" table in Schedule 3 will be marked "Yes".
- 8.13.3 The receiving party will be allowed to undertake whatever methods at their disposal to access and view the provided native file. No claim of privilege or confidentiality is waived by the providing party if the file contains such information.
- 8.13.4 The fields in Schedule 3 will be captured as near as practicable for password-protected documents.

9. Redaction of Privileged or Sensitive Customer Information Electronically Sourced Documents

- 9.1 Images or native formats of wholly privileged documents or documents wholly constituted of sensitive customer information will not be exchanged.
- 9.2 Objective data for wholly privileged documents or documents wholly constituted of sensitive customer information will be exchanged in the discovery lists only where it does not compromise the claim of privilege over the document.
- 9.3 File types listed in clause 8.10 that require redaction shall be rendered to text-searchable PDF format and have redactions applied, excepting Excel Spreadsheets, as per clause 9.4. All files that are converted to PDF for the purpose of redaction should retain all mark-ups, annotations etc as outlined in clause 8.5.
- 9.4 Where an Excel Spreadsheet requires redaction, a copy of that native document shall be redacted and that redacted copy will be provided. The method for redacting native format documents is as follows:
 - 9.4.1 The redaction is to be identified by inverse colour shade-marking the redacted part of the document along with the inclusion of text advising on the reasons for the redaction e.g. "Redacted for privilege" or "Redacted for sensitive customer information".
 - 9.4.2 If a party redacts a document in native format, then it must retain a complete version of that document in native format.
 - 9.4.3 Where practicable, all formulas or macros within a native document should be maintained in the redacted copy.
- 9.5 In the instance where an email or its attachments require redactions, both the email and its attachments will be rendered to text-searchable PDF format and redactions applied.

10. Exchange of Court Documents

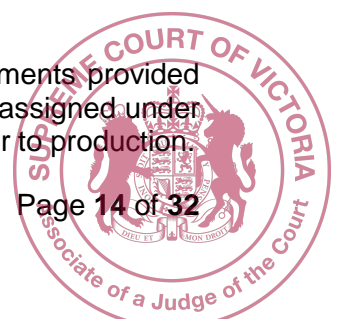
- 10.1 All documents filed with the Court are to be exchanged between the Parties.
 - 10.1.1 Expert Reports and affidavits are to be stamped with a Document ID after filing.



- 10.1.2 The Document ID will be in the format CCC.AAA.DDD.PPPP, where
 - 10.1.2.1 CCC is either EXP for an expert report or LAY for an affidavit
 - 10.1.2.2 AAA is the party code as per Schedule 1
 - 10.1.2.3 DDD is a sequential document number
 - 10.1.2.4 PPPP is a page number, which will commence at 0001 for each new document.
- 10.1.3 Similar Document IDs may be assigned to other court documents upon agreement.
- 10.2 Documents with a court stamp or signature are to be exchanged in Adobe Portable Document Format (PDF) only, showing the stamp and signature.
- 10.3 All other Court Documents are to be exchanged in multi-page PDF version 5, print enabled, selection of text and annotations enabled, unless the Parties agree to an alternative format.
- 10.4 Discovered documents referred to in court documents should be referred to by their full Document ID reference.
- 10.5 The naming convention of each file should reflect the witness name or pleading and the date filed or sworn/affirmed in Court.

11. Exchange of Subpoenaed Documents/Notice to Produce Documents

- 11.1 The party that applied for the subpoena (the Issuing Party) will process the subpoenaed material produced to the Court, in accordance with clauses 2, 3, 4, 5, 6, 8, and 11 of this Discovery Protocol.
 - 11.1.1 Where a party has requested “first access” to subpoenaed documents, this party will be responsible for the processing of the documents and costs associated.
- 11.2 The Issuing party will assign the material a party code that:
 - 11.2.1 Has not been assigned under Schedule 1 of this Protocol; and
 - 11.2.2 Easily identifies the producer of the subpoenaed material.
- 11.3 Once processed, the Issuing party will provide the processed material to the other party or parties at no cost.
- 11.4 The processed material is to be provided to the other party or parties within 14 days of the documents being produced under subpoena to the Court. In the event that this is not possible due to the volume of material produced, the Issuing Party will inform the other parties of this fact as soon as practicable and provide an estimated provision date.
- 11.5 The same process outlined above will be undertaken for documents provided under notices to produce, however the party code will be those assigned under Schedule 1, and the producing party will process documents prior to production.



12. Exchange of Large Volume Data types

- 12.1 Large volume data types (**LVDT**) include, but are not limited to:
 - 12.1.1 Bespoke or proprietary databases
 - 12.1.2 Bespoke or proprietary data models
 - 12.1.3 Bespoke or proprietary map or diagram systems
 - 12.1.4 Self-executing programs containing non-extractable documents (eg. a Java based multimedia report).
- 12.2 These data types are generally comprised of many individual components and files, which when processed individually are either unable to be imaged or the processing removes the interconnectedness required for the data source to function correctly.
- 12.3 Agreement should be reached between the Parties on the treatment of the LVDT, however generally:
 - 12.3.1 The LVDT is assigned a single Document ID in accordance with clause 3;
 - 12.3.2 The native version of the LVDT is provided to the other parties;
 - 12.3.3 In the event that proprietary systems are required to view the LVDT, these shall be provided.

13. Exchange of Chat, Instant Messenger records

- 13.1 Chat or Instant Messenger records include, but are not limited to:
 - 13.1.1 SMS
 - 13.1.2 MS Teams Chat
 - 13.1.3 Bloomberg Chat
 - 13.1.4 Slack, Google Hangouts etc
- 13.2 Insofar as this material can be captured and processed, the entire chat “thread” must be captured in xml, csv or json format, and produced in this form
- 13.3 Alternate methods for production may be agreed between the parties.

14. Quality Assurance

- 14.1 Each party shall use its best endeavours to ensure the accuracy of the data entry it provides.
- 14.2 After initial data and images have been exchanged between the Parties, if errors are found in data or images, the responsible Party should be notified and should re-issue the data or images, error free, in the agreed format.
- 14.3 If there are errors in images, only the appropriate images will be re-issued.
- 14.4 Minor errors in objective coding should be amended by individual Parties.



14.5 If more than 25% of an exchanged data set is incorrect then the disclosing party will reprocess that entire data set and reissue it to the other parties.

15. Privilege Clawback

15.1 It is assumed that all documents discovered by the parties have been reviewed for privilege prior to disclosure.

15.2 The parties agree that:

- a) the disclosure of any privileged material unless explicitly stated, shall be deemed to be inadvertent; and
- b) any inadvertent discovery of privileged material shall not result in the waiver of any associated privilege nor result in a subject matter waiver of any kind.

15.3 If, when reviewing another Party's discovered material, it becomes apparent to the Receiving Party that some of the discovered material may be privileged, the Receiving Party will:

- a) immediately suspend review of the apparently privileged material;
- b) not make copies of the apparently privileged material; and
- c) as soon as is reasonably practicable, notify the Producing Party of the disclosure of the apparently privileged material.

15.4 Upon receipt of a notification made pursuant to this section, the Producing Party will, as soon as is reasonably practicable or within five business days, either request the return of the apparently privileged material, or confirm that the disclosure of the apparently privileged material was intended. The Parties agree that if the Producing Party does not provide any response in accordance with this section, the disclosure of the apparently privileged material shall be deemed intended.

15.5 Upon receipt of a request for the return of the apparently privileged material, the Receiving Party will, as soon as is reasonably practicable and in any event within three business days, return the media containing the material to the Producing Party with confirmation that:

- a) all copies have been destroyed except to the extent that copies may exist by reason of normal backup procedures; and
- b) that the Receiving Party will not attempt to access any such copies.

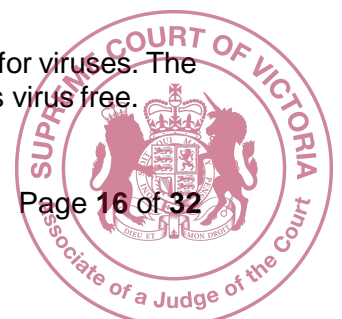
Upon return of the media containing the material, the Producing Party will issue a replacement copy with the privileged material removed or redacted.

15.6 If the Producing Party becomes aware that there has been an inadvertent disclosure of privileged information the parties will follow the steps outlined at section 15.3 and 15.5 above.

16. Virus Responsibility

16.1 It is the responsibility of the recipient of the electronic data to test for viruses. The sender will take all reasonable precautions to ensure that data is virus free.

17. Responsibility for Costs



- 17.1 It is the responsibility of each party to bear the cost of producing electronic data as outlined in this Protocol subject to any cost orders which may be made in the proceeding.

18. Updating or Adding Additional Data

- 18.1 Any updates should be accompanied by a covering letter outlining the affected Document IDs, detailing the information that has been amended and specifying any relevant instructions.
- 18.2 If additional data or images are found after the initial exchange, they should be exchanged in the format outlined in this Protocol.



SCHEDULE 1

PROPOSED PARTY CODES

PARTY	LEGAL ADVISER	ALLOCATED CODE
Nicos Andrianakis	Maurice Blackburn	NIN
Uber Technologies Incorporated Uber International Holdings B.V. Uber B.V. Uber Australia Pty Ltd Rasier Operations B.V. Uber Pacific Holdings B.V. Uber Pacific Holdings Pty Ltd	Herbert Smith Smith Freehills	UBR



SCHEDULE 2

HARDCOPY DOCUMENT FIELDS

19. Fields to be captured for documents sourced in hard copy, with respect to each of the four tables outlined in clause 2.1, are as follows:

19.1 **EXPORT TABLE**

FIELD NAME	DATA TYPE & MAXIMUM LENGTH	EXPLANATION
Document ID	Text, 21	The Document ID on the first page of the document according to the document numbering system.
Host Reference	Text, 21	First Document ID of the Host document where the document is an attachment. Each attachment should only ever have one host document.



FIELD NAME	DATA TYPE & MAXIMUM LENGTH	EXPLANATION
Document Date	Date, 11	<p>The date of the document as it appears on the document in the following format: DD-MMM-YYYY (e.g. 01-JAN-2011)</p> <ul style="list-style-type: none"> <input type="checkbox"/> Undated documents will have this field left blank. <input type="checkbox"/> If an accurate document date cannot be determined, an estimated date should be given and the Estimated field should be "Yes". • Date ranges cannot be used. The earliest date should be used, and the Estimated field should be "Yes". • If day is unknown, enter 01-MMM-YYYY, and the Estimated field should be "Yes". <input type="checkbox"/> If day and month are not known, enter 01-Jan-YYYY, and the Estimated field should be "Yes". <input type="checkbox"/> If the year is unknown, this field will be left blank, unless estimated date can be determined. <input type="checkbox"/> E-Mails: where there are multiple e-mails on one page, the date is the date of the first email that appears at the top of the first page. <input type="checkbox"/> Minutes of Meeting: Use the date of the meeting.
Estimated	Text, 3	To be left blank if a date is clearly evident on the document. A value of "Yes" will be used for estimated or partially dated documents.
Document Type	Text, 255	<ul style="list-style-type: none"> • See Schedule 4 for list of document types. • Document types not listed in Schedule 4 should not be used after document processing has commenced unless agreed upon between the Parties.

FIELD NAME	DATA TYPE & MAXIMUM LENGTH	EXPLANATION
Title	Text, 255	Used to provide an objective description of the document. Documents with no discernible title will have the value "Untitled"
Level_1		The Party level of the Document ID (see Clause 3.2)
Level_2		The Box level of the Document ID (see Clause 3.2)
Level_3		The Folder level of the Document ID (see Clause 3.2) under which the Searchable Images or Native Electronic Documents are stored.

19.2 **PARTIES TABLE**

FIELD NAME	DATA TYPE & MAXIMUM LENGTH	EXPLANATION
Document ID	Text, 21	The Document ID on the first page of the document according to the document numbering system.
Correspondence Type	Text, 9	One or more of the following 5 options identifying the type of person must be used: <ul style="list-style-type: none"> • To - for addressees • From - for authors • Between - for Parties to an agreement or other legal document (not correspondence) • CC - for additional people to which documents are addressed or authored • Attendees - for persons/organisations who attended a meeting.

FIELD NAME	DATA TYPE & MAXIMUM LENGTH	EXPLANATION
Persons	Text, 255	<p>Each person's name should be recorded as follows:</p> <ul style="list-style-type: none"> • Surname [space] First Initial [no full stop] (e.g. Bloggs J). • If a person is only identified by title and not by name, the title should be entered in this field e.g. General Manager • If there is a named organisation but no identifiable person for a document this field should be left blank • In relation to Emails, the display names or, if unavailable, the email address of the sender, recipient and persons carbon copied or blind copied into the e-mail.
Organisation	Text, 255	<p>The organisation to which the document relates to. Where there are multiple persons and organisations involved, the organisations are to be listed in correspondence with a relevant person.</p> <p>Organisations are to be entered as they appear on the face of document. Abbreviations should not be used.</p> <p>If there is a person but no discernible organisation, this field should be left blank.</p>

19.3 PAGES TABLE

FIELD NAME	DATA TYPE & MAXIMUM LENGTH	EXPLANATION
Document ID	Text, 21	The Document ID on the first page of the document according to the document numbering system.



FIELD NAME	DATA TYPE & MAXIMUM LENGTH	EXPLANATION
Image File Name	Text, 11	Where PDF files are created for each hardcopy document, the full name of the PDF file, including the file extension e.g. AAA.BBB.FFF.DDDD.pdf The extracted text file will include the full name of the text file, including file extension e.g AAA.BBB.FFF.DDDD.txt
Page Label	Text, 8	This is the file extension of the Efiles e.g. PDF.
Page Number	Number	This is a sequencing number.
Num_pages	Number	This is the number of pages in the document

19.4 **EXPORT EXTRAS TABLE**

FIELD NAME	DATA TYPE & MAXIMUM LENGTH	EXPLANATION
Document ID	Text, 21	The Document ID on the first page of the document according to the document numbering system.
The Category	Text	BOOL, DATE, NUMB, TEXT, MEMO or PICK
The Label	Text	The name of the field
The Value	Text	Field value for that document

An entry must be made in the Export_Extras table for the following fields for each document where they contain data:

LABEL	DATA TYPE & MAXIMUM LENGTH	CATEGORY
Redacted	<p>This field identifies whether document has been redacted or not.</p> <p>The permissible entries in this field are "Yes" or NULL</p>	BOOL
Sensitive Customer	<p>This field identifies whether a document contains sensitive customer information.</p> <p>The permissible entries in this field as "Yes" or NULL</p>	BOOL
Privileged	<p>This field identifies whether a claim of privilege is made over the document. The permissible entries in this field are "Yes", "No" or "Part" (for partly privileged documents).</p>	PICK
Basis of Privilege	<p>Description of the basis on which privilege is claimed:</p> <ul style="list-style-type: none"> • Legal Professional Privilege • Privilege, Without Prejudice • Privilege, Public Interest Immunity <p>Permissible entries are "LPP", "WPP", and "PII".</p>	PICK
Confidential	<p>This field identifies whether a claim of confidentiality is made over the document. The permissible entries in this field are "Yes" or "No".</p>	PICK

<p>Reason for Redaction</p>	<p>If a document has been redacted this field must be completed. It will need to be used where either:</p> <ul style="list-style-type: none"> • part of a document has been redacted; or • an entire document within a document group has been redacted. (A document group is a document that has one or more attachments). <p>The only permissible entries for this field are:</p> <p>Sensitive customer information – Part (for partly sensitive customer documents)</p> <p>Privileged – Part (for partly privileged documents)</p> <p>Only a subset of documents will have a Reason for Redaction.</p> <p>Parties may also indicate the reason for redacting a particular section of a document on the image, e.g, by stamping the redacted section "redacted for privilege", etc.</p>	<p>PICK</p>
-----------------------------	---	-------------



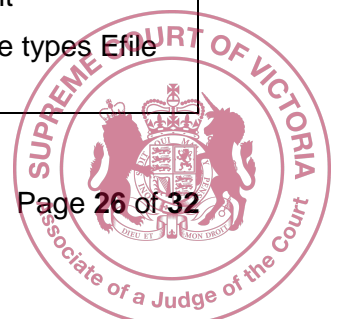
SCHEDULE 3

ELECTRONICALLY SOURCED DOCUMENT FIELDS

20. Fields to be captured for electronically sourced documents:

20.1 **EXPORT TABLE**

FIELD NAME	DATA TYPE	EXPLANATION
Document ID	Text, 21	The Document ID on the first page of the document according to the document numbering system.
Host Reference	Text, 21	For attachments to emails, the Document_ID of the host email is entered here. If an email is the attachment to another email, the Document_ID of the host email is entered here. For host documents or emails and non-related email Efiles, this field will be blank.
Document Date	Date, 11	For emails, the date will be extracted from the Date Sent field in the email. For Email Attachments and Efiles, the date will be extracted from the Date Last Saved field in the electronic file. Format will be DD-MM-YYYY The date is left blank where an email has not been sent.
Document Type	Text, 255	Email will be Document Type "Email". All other Efiles will be assigned document types based on the automatically assigned file types of the processing software (e.g. "Microsoft Excel Spreadsheet"). Parties should rationalise these document types into, eg: Email Microsoft Excel Spreadsheet Microsoft Word Document Parties should not use the types Efile or Email Attachment.



FIELD NAME	DATA TYPE	EXPLANATION
Title	Text, 255	For Emails, the Title field will be extracted from the Email's "Subject" field; where the Subject field is blank, the title will be left blank For Efiles or Email attachments, the Title will be the original file name of the Efile.
Level_1		The Party level of the Document ID (see Clause 3.2)
Level_2		The Box level of the Document ID (see Clause 3.2)
Level_3		The Folder level of the Document ID (see Clause 3.2) under which the Searchable Images or Native Electronic Documents are stored.

20.2 **PARTIES TABLE**

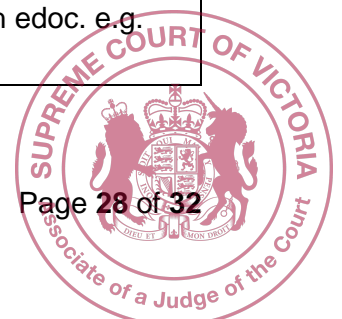
The Parties table will only contain data extracted from an email, since other electronic files do not have consistently reliable Parties' information.

FIELD NAME	DATA TYPE	EXPLANATION
Document ID	Text, 21	The Document ID on the first page of the document according to the document numbering system.
Correspondence Type	Text, 4	The following will be extracted from the email properties: a) "From" from the From field of the Email; b) "To" from the To field of the Email; c) "CC" from the CC field of the Email, and d) "BCC" from the BCC field of the

FIELD NAME	DATA TYPE	EXPLANATION
		Email.
Persons	Text, 255	<p>This will be extracted from the To, From, CC and BCC fields of each email as relevant.</p> <p>The full email address will be entered for each value extracted. Where possible, email groups should be extracted out to display their component parties.</p> <p>If a field is blank, no record will be generated.</p> <p>For chat records, this will be taken from the participants metadata</p> <p>For all other Efiles, this may be captured from the Author field</p>
Organisation	Text, 255	This field will be left blank, unless automatically captured

20.3 PAGES TABLE

FIELD NAME	DATA TYPE	EXPLANATION
Document ID	Text, 121	The Document ID on the first page of the document according to the document numbering system.
Image File Name	Text, 21	<p>Where PDF files are created for each Document, the full name of the PDF file, including the file extension e.g AAA.BBB.FFF.DDDD.pdf</p> <p>Where native files are captured for each Document, the full name of the native file, including the file extension e.g AAA.BBB.FFF.DDDD.xls.</p> <p>The extracted text file will include the full name of the text file, including file extension e.g AAA.BBB.FFF.DDDD.txt</p>
Page Label	Text, 8	The file extension of each edoc. e.g. PDF



FIELD NAME	DATA TYPE	EXPLANATION
Page Number	Number	This is a sequencing number.
Num_pages	Number	For multipage PDFs this is the number of pages in the document. For all other file types it will be 1.

20.4 EXPORT EXTRAS TABLE

FIELD NAME	DATA TYPE	EXPLANATION
Document ID	Text, 21	The Document ID on the first page of the document according to the document numbering system.
The Category	Text	BOOL, DATE, NUMB, MEMO, TEXT or PICK
The Label	Text	The name of the field.
The Value	Text	Field value for that document.

An entry must be made in the Export_Extras table for the following fields for each document where they contain data:

FIELD NAME	DATA TYPE & MAXIMUM LENGTH	The Category
Redacted	This field identifies whether document has been redacted or not. The permissible entries in this field are "Yes" or NULL.	BOOL
Sensitive Customer	This field identifies whether a document contains sensitive customer information. The permissible entries in this field as "Yes" or NULL.	BOOL
Privilege	This field identifies whether a claim of privilege is made over the document. The permissible entries in this field are "Yes", "No" or "Part" (for partly privileged documents).	PICK

Basis of Privilege	Description of the basis on which privilege is claimed: <ul style="list-style-type: none"> • Legal Professional Privilege • Privilege, Without Prejudice • Privilege, Public Interest Immunity Permissible entries are "LPP", "WPP", and "PII".	PICK
Confidential	This field identifies whether a claim of confidentiality is made over the document. The permissible entries in this field are "Yes" or "No".	PICK

FIELD NAME	DATA TYPE & MAXIMUM LENGTH	The Category
Reason for Redaction	<p>If a document has been redacted this field must be completed. It will need to be used where either:</p> <ul style="list-style-type: none"> part of a document has been redacted; or an entire document within a document group has been redacted. (A document group is a document that has one or more attachments). <p>The permissible entries for this field are:</p> <p>Sensitive customer information – Part (for partly sensitive customer documents)</p> <p>Privileged – Part (for partly privileged documents)</p> <p>Only a subset of documents will have a Reason for Redaction.</p> <p>Parties may also indicate the reason for redacting a particular section of a document on the image, e.g. by stamping the redacted section "redacted for privilege", etc.</p>	PICK

An entry must be made in the Export_Extras table for the following fields for each Efile where they contain data.

FIELD NAME	DATA TYPE	EXPLANATION
File_Path	<p>1 to 1</p> <p>This field will contain the relative directory source path as captured during data collection, including virtual folder structure from within an email repository file (e.g. fblogs\Inbox) or self-extracting container file (eg. ZIP file) where applicable.</p>	MEMO
File_Name	<p>1 to 1</p> <p>This field is extracted from the File Name of the Efile or Email Attachment</p>	TEXT



MD5	1 to 1 This field will contain the MD5 hash value for the electronic file	TEXT
-----	--	------



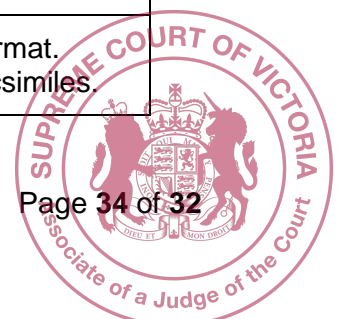
FIELD NAME	DATA TYPE	EXPLANATION
Password_protected	1 to 1 For electronic documents that are password protected, this will be marked "Yes".	BOOL
Non relevant system file	1 to 1 For automatically generated system files or embedded email signatures that are treated as attachments, this field will be marked "Yes"	BOOL
Erroneous Extraction Issue	1 to 1 Where embedded objects have been incorrectly listed as attachments to an email, but not produced, this field should be marked "Yes"	BOOL

SCHEDULE 4

LIST OF HARDCOPY DOCUMENT TYPES

NOTE: Additional document types may be required on a per case basis. Such additions should be signed off on by both Parties preparing data for exchange.

DOCUMENT TYPE	DESCRIPTION/EXAMPLE
Affidavit	
Agenda	Outline of meeting, business seminar or conference events scheduled to take place.
Agreement	Any document with multiple parties entering into an agreement including contracts, licences, trust deeds and statutory body agreements.
Brochure	
Business Card	
Certificate	Usually contains the word "certificate" in the title.
Chart	
Court Document	Exhibits, judgments, transcript of proceedings or any other document generated by or filed with a Court.
Diagram	Includes architectural plans, sketches or drawings. Also includes diagrams explaining how something works or operates. engineer's, architect's, or builder's drawings, plans, blueprints and aerial photographs of buildings or land.
Diary	
Drawing	
File Cover	A cover for a document that does not contain subsequent pages or Dividers such as tabs, separator sheets, etc.
File Divider	
Email	Any document that is in email format.
Extract	
Facsimile	Only applies to documents in the facsimile format. Documents with fax-tracks are not always facsimiles.



DOCUMENT TYPE	DESCRIPTION/EXAMPLE
Facsimile Transmission Report	Report containing receipt of facsimile. Usually a one page document containing information on when a fax was sent. Are also referred to as TX reports or Communication Reports.
Financial Document	Any document containing figures, pricing, budgets and cheques. This category does not include invoices, bank statements and statement of accounts or receipts.
Form	A document that requires another party to fill in certain fields e.g. questionnaires, application forms and timesheets.
Graph	
Notes	Any handwritten document. Handwritten diagrams or maps are not included in this category.
Invoice	Tax Invoices, Invoice of account, Bank Statements and Statements of account.
Letter	Should have an addressee and a signature line and will usually have a letterhead.
Licence	
List	List of names, addresses, index etc.
Manual	
Map	A hand-drawn or electronically produced map.
Memorandum	In-house correspondence within a company. Usually contains the word "Memo" or "Memorandum" in the title.
Minutes	Document containing attendees, discussions and action items that took place in a meeting.
Newspaper/Magazine Article	
Notice	
Photograph	Photographs.
Presentation	PowerPoint Presentation.

DOCUMENT TYPE	DESCRIPTION/EXAMPLE
Quotation	
Receipt	Includes receipts of transactions, packing sheets and delivery notes.
Report	Documents providing research, analysis or reports on a finding or event.
Table	Documents containing information in a table or .xls format. Any table/spreadsheets containing pricing, budgets, monetary values etc should be financial documents, not table/spreadsheet.
With Compliments Slip	