TOTSCo Bulletin No 18

DATE: 14 July 2023

SUBJECT: Responses and Conclusions to Request for Feedback on Data Reporting Bulletin No 5

We recently requested your views on the reporting, to industry and Ofcom, of data from the TOTSCo hub for the purpose of monitoring the OTS process (see Bulletin 5, https://totsco.org.uk/wp-content/uploads/2023/04/Bulletin-No-5-Data-Reporting.pdf, dated 14th April).

TOTSCo supports the reporting of this data, and we asked for your views including, but not limited to:

- Whether TOTSCo should supply Ofcom with the suggested information
- Comments on the reasons that we gave for supporting the proposal
- Measures that would help give confidence in the appropriate handling of such information
- Any alternative or additional suggestions for OTS monitoring

We undertook to publish the results of this exercise, and to propose a way forward.

Summary of Responses

We received 15 responses.

Nine respondents agreed that TOTSCo should generate and report on such data and had few or no or concerns. Where they gave reasons, these largely echoed those given by TOTSCo in Bulletin 5.

Two respondents were content for data to be shared with Ofcom but preferred this to be done by the hub vendor rather than by TOTSCo, citing data minimisation.

Four respondents were against the sharing of confidential information altogether. The concerns that were cited included:

- No commercially confidential information should be supplied to any party, including Ofcom
- Commercially confidential information may be inadequately protected, or leaked
- The necessary security measures will add to complexity and cost.

Larger respondents were more favourable to the proposed data reporting. Please see the Appendix for more detail on all responses.

What measures would help give confidence in the appropriate handling of such information

Several respondents asked to see more detail on TOTSCo's security policy and data-protection schedule.

Some responders commented that end to end encryption would give them more confidence in data security.

Alternative Suggestions and other Comments

Some respondents suggested that they could make submissions directly to Ofcom without TOTSCo involvement.

Some CPs requested the implementation of a dashboard that would allow them to monitor the Hub's health and status.

Consideration and Conclusions

While the responses were largely aligned with the principle that the data should be shared as proposed with Ofcom and industry to monitor the OTS process, some respondents expressed concerns about the security of commercially confidential information and others were opposed to the principle that data should be shared. There is also a broad wish to understand more about TOTSCo's arrangements to ensure that data is kept secure and that access to it is restricted.

We considered the suggestion that the reports should be provided directly by the hub vendor. We believe that delegating the production of data to the hub vendor would introduce additional complications and costs and raises issues of governance and accountability. Furthermore, TOTSCo will implement the required security measures regardless of the reports that we produce, given our potential access to personal and commercially confidential data. For these reasons we believe that TOTSCo is better placed than Tech M to perform this function.

To help give industry the confidence that it needs around the handling of commercially sensitive information, TOTSCo will circulate for comment, around the end of August, three relevant policies (see below) that will then be incorporated into the User Agreement. These policies cover the data-access controls within TOTSCo and the hub, and some technical and organisational security details. We also propose that one year after OTS go-live, or sooner if substantial issues arise, we review the operation of these policies, and invite feedback from industry on the operation of reporting data to the regulator and to industry.

TOTSCo will, therefore:

- Design and implement the appropriate reports for sharing with industry and with Ofcom for implementation after OTS go-live.
- Circulate for comment, in advance of the User Agreement publication;
    - Security Policy
    - Data Protection Schedule
    - Analytics, Reporting and Metadata Access Control Schedule.
- Consider the requests to publish metering and operational information.
- Schedule a review of the reporting to Ofcom and industry, one year after OTS go-live.

TOTSCo

July 2023

Appendix 1 – Summary of Responses

Whether TOTSCo should supply Ofcom with the suggested information	**Comments on the reasonings given in this note**	**What measures would help give confidence in the appropriate handling of such information**	**Any alternative or additional suggestions for OTS monitoring**	**Other Comments**	
The data points outlined in the bulletin are acceptable. o Any data points that contain both the sending and recipient CPIDs MUST not be provided to any party. This kind of telemetry SHOULD be considered commercially sensitive information. Information containing the contents of messages (other than type and error codes) SHOULD NOT be provided to any party. This kind of telemetry MUST be considered commercially sensitive information.	The leaking of commercially sensitive information can be used to influence competition in the UK.	Providing transparent access to the data submitted to Ofcom on behalf of a CP. Allowing a CP to opt-out of automated reporting on their behalf to Ofcom.	A CP can submit directly to OFCOM. (We already are providing recurring reports in relation to the services we are provided to a given property, and so OFCOM do not need this information from TOTSCo).		R1
[We] agree in principle with the proposals to share information with Ofcom as this will provide Ofcom with a good view of how well the overall process is working, as well as whether CPs appear to be following the process correctly. We believe that once the suite of reporting to Ofcom is agreed, any further changes / additions are					R2

discussed with Industry before being implemented					
This respondent requested confidentiality					R3
This respondent requested confidentiality					R4
[We] agree with TOTSCo submitting the reporting information from source into Ofcom but we expect the following when such information is shared from time to time. - CPs are required to be notified of this. When TOTSCo shares or reports on any information related to [us], the same must be shared with [us] as well for our information. - Industry aggregated information to be shared with [us] - providing us copy of the data shared with Ofcom - Helping us understand where [we] are as compared to other CPs (by anonymising industry data)		[We] would like TOTSCo to provide assurance that such data is encrypted while at rest and only authorised individuals have access to this information. TOTSCo to share governance process the information is accessed by the people. Who will be able to review and sign it off ? Please confirm where this information will be held ? Any inadvertent disclosure should be notified to the CPs	Hub response times Net number of switches Message delivery timeouts		R5
We do not have a strong position on the matter, and are generally content for the Hub to provide reports on usage to Ofcom.					R6

No customer data (name, address, email, phone, service…) and therefore no reporting should be possible otherwise it creates issues with GDPR and security. It would break the proposed End to End encryption proposal. No provider data which are commercially sensitive (churn between providers, volume between providers…) should be shared with OFCOM and should be recorded/visible to TOTSCo otherwise this information could be used for marketing, sales, and other activities to impact competition in the U.K. Metering data: Hub performance, success/failure without CP ID is acceptable (nothing commercial sensitive) It is important to note that the more TOTSCo try to do, the more expensive it becomes for CPs and ultimately broadband subscribers	If customer data and provider data is shared with OFCOM and stored with TOTSCo it would break E2EE encryption AND would be commercially sensitive data that can be used to impact competition in the U.K.	1. Limiting to metering data 2. Giving option to CP to report directly to OFCOM if they want to/are asked to 3. Accept E2EE encryption	1. CP can report directly to OFCOM (if requested) more data but currently we are already reporting to OFCOM 2. TOTSCo should limit to metering data (as described above)		R7

In terms of the information requested, we have no objection to this being provided to OfCom. In terms of whether TOTSCo should supply it, we see no reason why it can't be supplied by the hub vendor and so there's no need for TOTSCo to be involved.	A general comment is that there's no reason for TOTSCo to have access to this data – instead, Tech Mahindra provide it directly to OfCom rather than OfCom via TOTSCo. This could be reporting in the hub (with appropriate security, auditing, etc) solely available for OfCom to use or Tech Mahindra could provide it directly.Regarding the specific points:• On point 1, agree it is in wider interest of all CPs that OTS is monitored, but do not agree it has to be TOTSCo that does ito It's worth noting there's no reason the general health of the OTS process can't be made available to all of industry, and OfCom, by the hub vendor• On point 2, agree it is time-saving for CPs but only to a degree as CPs will most likely want to produce this same information themselves for review and monitoringo It would be far more beneficial for the hub to provide the same set of reports OfCom	We believe it's better to let OfCom go to the hub (or vendor) directly, but if they were going to TOTSCo then the following would give confidence:• Regular audits with transparency of findings• Seeing the proposed technical and process measures, data retention and training policies• Seeing the contractual terms with the vendor around their technical and process measures, data retention and training policies, security and confidentiality measures• Strong contractual penalties with the vendor for breaches• Strong penalties to TOTSCo for breacheso Strong penalties to any CP involved (e.g. if passed information or a CP's employee that has a role at TOTSCo is involved)	Make it the responsibility of the hub vendor, and it becomes part of the contract (including keeping such data confidential like they must already do with PII data).Tech Mahindra will have all this data anyway, so there must already be (or, if not, need to be added) contractual clauses around technical and process measures, data retention, security and confidentiality, GDPR, etc.With regards to the E2EE encryption consultation, having the entire message be encrypted would, of course, prevent the hub vendor from providing this information, but it would remove all concerns around TOTSCo's handling of this data and CP's would need to produce the data as requested by OfCom.		R8

	would get to each CP (except that the CP reports would only be for messages sent or received by that CP)• On point 3, agree the process refers to providing information to OfCom but note it was only recently that OfCom have even said what this would be and how it was to happen was an open questiono Traditionally OfCom has gone separately to individual organisations• On point 4 it is simpler to not let TOTSCo have access to this information at allo This avoids the need for, and cost of, extra technical or process measures and auditing of such				
We agree with the importance of reporting hub related information to industry and understand Ofcom's interest in the subject. We are happy for TOTSCo to provide the information to industry and Ofcom subject to TOTSCo putting in place robust processes around data processing, data retention and management of access					R9

to the data. We consider that irrespective of the encryption method chosen, TOTSCo should be able to provide the relevant data to industry and Ofcom. If TOTSCo were unable to provide the data, then [we] will be able to provide the information to TOTSCo and/or Ofcom itself.					
Ofcom should have access to the same TOTSCo data as any other member of the public. As noted in the discussion paper Ofcom has legal powers to request further data from individual CPs should they want to.	Holding private or confidential data within the hub increases the complexity of the hub and the services and policies associated with the hub. For example, maintaining confidentiality agreements, maintaining user accounts and access controls to the data etc. If all data held by the hub is available as public information, then much of this complexity is removed.	TOTSCo should make clear to CPs that it is committed to its value of transparency and so any data stored by the hub will be publicly available. Given this perspective it is likely that CPs and Ofcom may want to change their view on what data should be stored in the hub	The TOTSCo decision on what data to store in the hub provides an opportunity to re-commit to its value of transparency. If there are valid reasons why any data stored by the hub cannot be made public then the hub should not store it.		R10
[We] agree with TOTSCo's position that, as provider of the central switching platform, it is well positioned to gather data on the functioning of the One Touch Switch process. We agree that this is a role that TOTSCo should play and believe that this					R11

delivers benefits to both CPs and Ofcom (in terms of saving cost through ease of information provision). As TOTSCo notes, it needs to ensure it puts clear and rigorous processes in place to ensure that CP confidential information remains protected. These processes should be appropriately documented to give CPs confidence that the information will remain confidential and only accessed by those within TOTSCo who are subject to the relevant NDA and have no affiliation to any particular Communications Provider. The above feedback is (obviously) subject to the data encryption policy implemented by TOTSCo allowing them visibility of the relevant data that Ofcom wishes to have access to.G20					
This respondent requested confidentiality					R12

We do not support TOTSCo generating aggregated operational data regarding switching. We are concerned over the confidentiality of our data, and are not happy that any level of internal control will guarantee this.Instead, we believe that only Tech Mahindra ('TM') should generate operational switching data, both at an aggregated industry level, and for each Hub user. TOTSCo should not have visibility of anything that an individual operator cannot see.We believe that TM should be able to provide all the metrics asked for by Ofcom. We think it unlikely that Ofcom would seek data from individual Hub users, as TOTSCo suggests, given the complexity of doing this. We think instead, they will go straight to TM for their data needs, in the same way that they issue s135s Information Requests to Syniverse from time to time in the mobile industry, rather than going to individual operators and seeking data themselves.Our view is that					R13

TOTSCo providing this information to Ofcom – when TM can do it perfectly well – is duplication, doesn't meet data protection requirements for data minimisation and creates unnecessary confidentiality risks.					
We think this should come from TOTSCo because it ensures the right level of consistency and availability of the data for Ofcom. We really do not want to be encouraging Ofcom to be making formal data requests to CPs directly if we can avoid it. I also think it will help ensure that our own data and reporting capability is appropriate from day 1.		We think that TOTSCo should publish the steps they are prepared to take at the earliest opportunity to give CP's confidence. We don't believe this should be a major issue given people like Openreach have been capturing data from multiple providers and managing it without any problems.			R14
[We] are comfortable with the proposed format for TOTSCo reporting data to Ofcom as outlined in the request for feedback. We assume in this regard that TOTSCo would be using an accepted industry format for sharing the data (i.e. via the Ofcom FTP platform or similar arrangement with adequate security safeguards).					R15