Safari Mobile (UK) Ltd
Response to Consultation on
PSA Guidance on the Retention of Data

Background

Although it makes sense for the PSA to present Question 1 first to confirm that everyone is talking about the same thing, we will answer Question 1 last as I believe our answer there is informed by our answers to previous questions.

Q2. Do you agree that two years is an appropriate period for all Relevant Data to be retained as standard, to enable sufficient time for (i) commencement and progression of PSA enquiries and determination of appropriate action and (ii) resolution of complaints and/or concerns by network operators and providers? If not, why not?

The EU General Data Protection Regulations 2016 (GDPR) did not dramatically change the legal requirements around data protection. However, they have heralded a dramatic change in the way people think about data protection. In the past, the working standard was that data should be retained for as long as it was possible for that data to have any value whatsoever. The new mindset is to retain data only as long as it is required for its principle purposes.

Perhaps we should go further. Perhaps we should say that holding personally-identifiable data unnecessarily causes consumer harm in and of itself. I think we can all agree that there is the potential for consumer harm – the data being hacked, the data being misused. However, time and again data has been hacked and misused and therefore perhaps we should simply resign ourselves to that fact that holding data is a harm.

The Limitation Act 1980 sets the ordinary time limit for contract disputes at 6 years – from the last "accrual of cause", not from the data of the contract. Imagine that a consumer join a PRS subscription in 2010 and cancels that subscription in 2014. In the strictest interpretation of the Limitation Act, the PRS provider could have a legitimate interest in retaining proof of consent to charge unto 2020 – that being 6 years after the last successful charge in 2014.

In light of the change in mindset heralded by GDPR, we are minded to not adopt this broadest interpretation of legitimate interest. Instead we are inclined to rely on a reasonability / balance of probability defense.

The outline reasonability argument will be that (1) the sums involved are sufficiently small, (2) the industry is sufficiently well regulated, and (3) the privacy interests of consumers are sufficiently strong that we do not retain individual evidence of consent to charge for that long.

The outline balance of probabilities argument is that the industry is sufficiently regulated that if our consent to charge process was flawed, this would have been discovered. Since there are no PSA concerns about our consents to charge, then on the balance of probabilities a judge should accept our assertion that a particular consumer did consent to charge.

With these in mind we now turn to Question 2: Is two years the correct duration for the requirement to retain Relevant Data?

First, we note that the PSA is making no reference to any accrual of cause. In other words, if a user joins a subscripion in January 2017, has not stopped that subscription, is still being billed today, but the PSA has not opened an Investigation of the service in question, then we are free to delete the evidence of consent to charge.

Is this reasonable? I think so. From the PSA's perspective, the PSA is investigating the service not the experiences of individuals. If a service is still operating and is non-compliant then there will be more recent evidence of non-compliance. The loss of evidence in this specific instance should not be material.

If the service is no longer operating, then, if it had any suspicions, the PSA will have had sufficient time to open an Investigation (which preserves the evidence). If suspicions about the consent to charge process have not arising within two years of the last time that process was used, then it is hard to imagine what new developments could occur to raise such suspicions, and therefore it is reasonable to lose the evidence of consents to charge.

From the L2's perspective, this thinking feeds into the balance of probabilities defense. Yes, we do not have evidence of the consent to charge for this particular person; however, no issues were found by the PSA around our consent to charge process. Indeed, no suspicions were raised by the PSA around the consent to charge process. Therefore, on the balance of probabilities, the consumer consented.

So, the first part of our answer is that we agree the time limit should be absolute and should not cascade back from the last accrual of cause.

The second part of Question 2 relates to the term of two years. This is more subjective. In essence, how long is it reasonable for the PSA to get sufficiently suspicious to launch an Investigation? The PSA lists 4 scenarios on page 6 as to why such suspicions may be delayed.

The first thing to remember is that the theshold to launch an Investigation is pretty low. And, once an investigation is launched, Relevant Data cannot be deleted even once it is more than two years old. Keeping this in mind, I have the following reactions to the 4 scenarios.

The first scenario involves initially there not being sufficient concern to open an Investigation but over time concerns mount and then an Investigation is launched. Although a valid scenario, I refer to my point above. The PSA is investigating a service not the experiences of any particular individual. If concerns mount, then likely the service has continued operating. Although old evidence might expire, it will have been replaced by new evidence that is more compelling. So, what is the harm (to the investigative process) if the particular old (and unconvincing evidence) is lost?

The second scenario involves the Investigation spanning multiple services. Again I refer to the principle laid out above. If an issue is a continuing concern, then there is fresher evidence available. If a current concern can be retroactively applied to a service that was stopped a good while ago, what is the regulatory or investigative benefit in being able to retrospectively investigate that old service?

The third scenario involves the refusal of a provider to cooperate during the enquiry phase. Is this concern not better served by lowering the threshold by which an Investigation is launched … especially in the case of non-cooperation? Remember that once an Investigation is launched, Relevant Data must be retained.

The fourth scenario involves complex value chains. Is this concern not better served by lowering the threshold by which an Investigation is launched – in the case of complex value chains – and quickly spreading said Investigation to cover all members of the value chain involved in the service?

One can imagine a scenario where (say) a front L2 hides the identity of the real service provider. In this scenario, is the ability to investigate the service itself impeded by this fiction? I think not. I think the PSA is perfectly able of establishing that the service itself is in breach completely independently of being able to identify the true parties responsible.

What I am getting at is that I think two years is too long. I think one year of retention is sufficient.

If the service is still operating, then fresh evidence will be available. If the service has not operated for a year, then it is hard to imagine suspicions increasing after one year of discontinuation.

For the avoidance of doubt, let me address part (ii) of this question. I believe that the PSA investigating a service and finding it in breach is a sufficient remedy for everyone who has ever complained about a service, regardless of whether the individual circumstances of each complainant are known … keeping in mind that we are talking about the very narrow case of a service operating for more than two years, where suspicions did not arise at the start of the service but have arisen more recently, and the service has been found in breach and the appropriate remedies imposed.

What I am getting at is that the resolution of individual complaints does not require evidence of the specific circumstances of every complainant.

Q3. Do you agree that three years is an appropriate period for all Relevant DDRAC Data to be retained as standard, so as to enable sufficient time for (i) commencement and progression of PSA enquiries relating to DDRAC and determination of appropriate action and (ii) resolution of concerns by Level 1 providers and network operators? If not, why not?

I understand and agree with the logic that Relevant DDRAC Data should be held for longer than Relevant Data. Given that the pool of data subjects affected is (1) dramatically smaller and (2) involves people who have chosen to participate in the PRS industry, and (3) likely key elements of the Relevant DDRAC Data will get updated periodically, I have no objections to retaining this data for three years.

Given (3) above, I do not see why the data needs to be held for longer than three years.

Q4. Do you agree that all Relevant Data and Relevant DDRAC Data should be retained throughout the lifespan of an investigation? If not, please explain why.

I understand and agree with the logic that evidence must be retained during an Investigation. However, one should keep in mind that the PSA is free to retain its own copy of evidence even after the subjects of an Investigation have deleted that data.

So, in essence this question relates to the duration of the period of Discovery. Regardless of procedural obstacles, is it reasonable for Discovery to continue indefinitely? I think not.

The Limitation Act sets 6 years as the limit to bringing action for contractual matters. I would suggest that the PSA should be required to discover all relevant evidence within 6 years even if the underlying Investigation gets bogged down in procedural arguments.

In addition, to avoid abuses of process I think the PSA should monitor the opening of Investigations, their ultimate disposition, and the duration that they are open – to ensure that Investigations are not being opened or are not being dragged out inappropriately merely to retain evidence – which, as detailed above, harms consumers.

Also, the PSA should monitor progress on an Investigation. If insufficient progress is being made on a particular Investigation (not due to active obstruction), then that Investigation should be closed. The PSA should monitor the forward momentum of each Investigation.

Q5. Do you agree with our assessment in relation to the GDPR considerations? Is there anything else in terms of GDPR that we should take into account?

We note that you have placed the PSA's data requirements into two groups: Relevant Data, and Relevant DDRAC Data. We question whether this grouping is appropriate. Perhaps there are five types of Relevant Data:

(1) evidence of consent to charge
(2) evidence of supply of required system messages
(3) service content – categories (a), (b) and (j) on page 8
(4) merchant-to-consumer communications about the service – categories (d), (e) and (f)
(5) evidence about the service provider – categories (c), (g), (h) and (i)

Given that the main complaint made to the PSA is that users did not sign up to the service in question. There is logic in retaining (1) – evidence of consent to charge – for two years. By extension, there may be logic in retaining (2) – evidence of price warnings, etc.

We question the need for (3) – service content – as this is likely to be the most intrusive and of the least value. For example, imagine a person-to-person dating service. Under what circumstances would the PSA need to see the text of messages between consumers?

On page 8 some scenarios are provided – e.g. adult content being provided to underaged users. This consumer harm, however, may be addressed by a data retention requirement applying only to adult services.

Another scenario on page 8 is that the service provided may not match the description given pre-purchase. Is this not something that the PSA can obtain from the complainant? Perhaps the complainant will not have retained evidence of the promotion (and so the PSA can require merchants to retain this) but perhaps it is reasonable for the consumer themselves to have their own evidence if they are going to assert that they were misled as to the content of the service.

Q1. Do you agree with the non-exhaustive data sets listed within Annex A?
If there is anything that you consider should be added to, or removed from, the list please explain why.

As discussed in our answer to Q5, we believe that the Relevant Data can be split into separate sub-categories. We suggest that the data in certain sub-categories may not need to be retained at all.

The description of the data in Annex A is around format and source, and not content and therefore does not lend itself to the sub-categories described above.

As to the actual content of Annex A, we question the wording of Bullet 3(3) - “Timestamped screenshot records of served browsing pages”.

What is relevant here is what the user saw. What the user actually saw depends on their device and settings on their advice. Therefore any “screenshot” (i.e. a pictorial composite of what was presented to the user) will be a best guess recreation, even if created at the time. What is more important is the actual HTML code and collateral sent to the user's device – which is distinct from Bullet 3(2) – which is the meta-code used to create the actual HTML code and collateral sent to the user's device.

Q6. Having considered the proposals in this consultation do you agree with the proposed Guidance at Annex A of this document? If not, why not?

Other than the amendments proposed above, we agree with the proposed Guidance.