THE PRACTICAL NOMAD

EDWARD HASBROUCK

1130 Treat Avenue, San Francisco, CA 94110, USA
phone +1-415-824-0214
edward@hasbrouck.org
https://hasbrouck.org

The Practical Nomad: How to Travel Around the World
The Practical Nomad Guide to the Online Travel Marketplace
Avalon Travel Publishing (Perseus Books Group / Hachette)
https://practicalnomad.com

"The Practical Nomad" books and Web site are written by union labor:
Member, National Writers Union (UAW Local 1981, AFL/CIO)

10 December 2018

European Commission
Directorate-General for Mobility and Transport (DG-MOVE)
1049 Bruxelles/Brussel
BELGIUM

by e-mail: MOVE-CRS-EVALUATION@ec.europa.eu

Comments re: Public consultation on the evaluation of the regulation on a code of conduct for computerised reservation systems <https://ec.europa.eu/info/consultations/2018-crs-code-conduct_en>

The comments below are submitted to supplement my response to the questionnaire at <https://ec.europa.eu/eusurvey/runner/2018-CRS-Code-of-Conduct> and to raise issues related to the CRS Code of Conduct not addressed in the questionnaire.

These comments are submitted in my individual capacity as an expert in the implications of CRS design, operation, and usage for privacy, data protection, and other human rights. They do not necessarily reflect the views of any of the organizations with which I am affiliated, my employers or consulting clients, or the publishers of my work.

I have worked as a front-line travel agent and CRS user, as a manager of CRS contracts and operations and trainer of travel agents in CRS usage, as a subject-matter expert in the development of online travel agency expert systems and business process automation software that interfaces and exchanges data with CRSs, and as a journalist and consumer advocate with a special focus on CRS privacy and data protection issues.

One of my articles on the content, sources, uses, and privacy implications of data stored in CRSs won a Lowell Thomas Travel Journalism Award for investigative reporting from the Society of American Travel Writers Foundation. I have testified as an invited expert witness on this issue before the LIBE Committee of the European Parliament[1], the Canadian Parliament[2], and the Advisory Committee for Aviation Consumer Protection of the U.S. Department of Transportation[3]. My work in this field is frequently cited in academic research and by other journalists, and I have been consulted on these issues by numerous U.S., European, and international nongovernmental organizations.

I share the concern of other consumer advocates that the CRS Code of Conduct remains – along with the requirement for each airline to publish and comply with a tariff of fares – a key means of ensuring transparency and non-discrimination in airfares. CRSs facilitate comparisons shopping, in the face of airlines' efforts to make it more difficult for consumers to compare prices and to replace fare tariffs with personalized prices.

Airlines don't want transportation to be commodified. Airlines don't want the services of Airlines A, B, C, and D in providing a bundle of services including transportation of 1 adult person and 2 pieces of checked luggage from Point P to Point Q to be regarded as fungible. But travellers do, in fact, regard air transportation as a commodity, and regard most airlines as fungible. Airbuses are Airbuses, and Boeings are Boeings, regardless of what logo is painted on the tail. Travellers want to compare prices, and CRSs that provide neutral displays are the best means available for them to do so.

The CRS Code of Conduct also includes significant and necessary – although to date unenforced – protections for the highly sensitive personal information about travellers stored in CRSs. These provisions of the CRS Code of Conduct should be retained and enforced, for the same reasons that were discussed in comments to the Commission by the Identity Project[4] in 2007, the last time the CRS Code of Conduct was reviewed.

The privacy and data protection provisions of the CRS Code of Conduct:

1. Should be retained, regardless of what other changes are made to the Code of Conduct;
2. Should continue to explicitly define CRSs as data controllers, regardless of what other entities might also be considered controllers of the same data; and
3. Should be enforced, both now and in the future, including by requiring CRSs to:
   (a) Replace "record locators" with user-selectable, user-changeable passwords, and
   (b) Add immutable access logs, similar to the current change logs, to PNR "histories", to enable CRSs and CRS users to provide data subjects with an accounting of disclosures and international transfers of PNR data and to enable oversight of purpose and geographic access controls.

---

1 Links to archived video and annotated slides available at <https://hasbrouck.org/blog/archives/001855.html>
2 Links and excerpts from transcript available at <https://hasbrouck.org/blog/archives/001903.html>.
3 Links to slides and additional references available at <https://hasbrouck.org/blog/archives/002071.html >
4 Available at <http://hasbrouck.org/IDP/IDP-CRS-comments.pdf>

Although two of the three largest CRSs operating in the European Union are based in the U.S., there is still no U.S. privacy or data protection law applicable to data held by CRSs. There is no general U.S. Federal privacy or data protection law for commercial data. There is no sector-specific U.S. Federal privacy or data protection law applicable to travel reservation data. Any U.S. state regulation of CRSs, including any state privacy or data protection law applicable to airline reservations, is preempted by U.S. Federal law.

In the U.S. context, some of the consumer privacy and data protection issues with data held by CRSs were discussed in comments I filed with the U.S. Federal Trade Commission in 2009 in conjunction with the Consumer Travel Alliance, the Consumer Federation of America, and the Center for Financial Privacy and Human Rights.[5]

In the absence of any applicable U.S. privacy or data protection rules, the E.U. CRS Code of Conduct remains essential to protect the subjects of CRS data.

The only mention of privacy or data protection in the European Commission's questionnaire for this consultation is a question as to whether "the provisions of the CRS Code of Conduct are coherent with the policy approaches or objectives underlying… The EU's General Data Protection Regulation (Regulation (EU) 2016/679)."

The privacy and data protection provisions of the CRS Code of Conduct are consistent with the GDPR. But that does not mean that the GDPR is an adequate substitute for the privacy and data protection provisions of the CRS Code of Conduct, or that those provisions of the CRS Code of Conduct are no longer needed.

The privacy and data protection provisions of the CRS Code of Conduct were retained and strengthened when the Code of Conduct was last amended in 2009 – long after the E.U. Data Protection Directive had come into effect. For the same reason that these provisions of the CRS Code of Conduct were needed to supplement the Data Protection Directive, they remain necessary to supplement the GDPR to take account of the special features of CRSs and the special difficulties these pose for data protection.

The problems that data subjects and regulators would would face in assigning responsibility for responding to subject access requests, if the privacy and data protection provisions of the CRS Code of Conduct were repealed, are made clear by the contradictory statements made by the different CRSs as to their GDPR responsibilities.

Travelport says that: "Travelport's role as to GDS operations has been decided via European regulation, specifically, Regulation 80/2009 on a code of conduct for computerised reservation systems. Commonly referred to as the CRS Code of Conduct, this regulation explicitly states that a computer reservation system operator, such as Travelport, is considered a data controller for those types of operations."[6]

5 Available at <https://hasbrouck.org/articles/Hasbrouck_et_al-FTC-6NOV2009.pdf> or at <https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00025/544506-00025.pdff>

6 "Travelport and GDPR: A summary of how we are complying", <http://traveloneinc.com/wp-content/uploads/2018-02-Travelport-GDPR-Statement.pdf >

On the other hand, Sabre does not mention the CRS Code of Conduct, and as a consequence, reaches the opposite conclusion: "Is Sabre considered a processor or a controller? Sabre is considered a processor for the majority of its services. Sabre's customers and travel suppliers are considered controllers, and thus have responsibility for the requirements imposed on controllers under the GDPR."[7]

Amadeus has not made a clear statement of whether it considers itself a data controller, a processor, or both, or for which data it considers itself a controller.

The difference between the interpretations by Sabre and Travelport of their responsibilities with respect to data protection makes clear that, in the absence of the definition of CRSs as data controllers in the CRS Code of Conduct, CRSs will try to claim that they are merely processors and not controllers of personal data. And if even Travelport and Sabre can't agree on whether they are controllers or processors, that is strong evidence that this needs to be made explicit in the CRS Code of Conduct.

A typical Passenger Name Record (PNR) stored by a CRS can contain information related to multiple travellers and non-travellers[8], and to travel services provided by multiple companies through multiple intermediaries.[9] Without this provision in the CRS Code of Conduct, it would be difficult to assign responsibility for data protection with respect to much of the data held by CRSs. Consumers seeking to exercise data protection rights would be sent – as they often are today – on a "wild goose chase" from one company to another, each pointing the finger at a different company as the data controller, or simply disclaiming responsibility for being the data controller.

This is exactly why the provision defining CRSs as data controllers – regardless of what other entities might also be considered controllers – was included in the CRS Code of Conduct. It was essential, and it remains essential. It should be retained, regardless of what changes are made in the CRS Code of Conduct, and it should be enforced.

There has been no enforcement of the privacy and data protection provisions of the CRS Code of Conduct, despite complaints by consumers and data subjects.

The reasons why there haven't been more such complaints include that data subjects are rarely told that their data has been transferred to a CRS, or to which CRS or CRSs (a single reservation can result in PNRs being created in two or three CRSs) and that the Commission has not advertised how or to whom complaints should be made.

Despite attempts by Members of the European Parliament and by staff of other E.U. institutions to assist me, it took me more than five years to find a point of contact at the Commission that would accept a complaint of violations of the CRS Code of

7 "GDPR Frequently Asked Questions", <https://www.sabre.com/about/privacy/gdpr-faq/>

8 See the list of some of the categories of non-traveller subjects of PNR data in the 2007 comments to the European Commission by the Identity Project, available at <http://hasbrouck.org/IDP/IDP-CRS-comments.pdf>

9 "What's in a Passenger Name Record (PNR)?", <https://hasbrouck.org/articles/PNR.html>

Conduct.[10] The Commission should add a page to its Web site informing consumers and other subjects of PNR data of their right to lodge complaints of violations of the CRS Code of Conduct with the Commission, and specifying the point of contact for such complaints.

My complaint has now been pending for more than 18 months.[11] In February 2018, I received a message from DG-MOVE, "We are currently still assessing your complaint but I hope that we will be able to give you a reply on the substance of your complaint in the coming weeks." But 10 months later, I still have received no notice of any action on my complaint, and no response to recent inquiries as to the status of the investigation.

None of the CRSs have ever implemented the technical measures – including replacing or augmenting "record locators" with user-selectable and changeable passwords, and adding immutable access logs to the change logs in PNR "histories" – which would be necessary in order for CRSs to comply with the CRS Code of Conduct, or for CRSs or their users to comply with the Data Protection Directive or the GDPR.

As long as the Commission refrains from, or delays, enforcement of the privacy and data protection provisions of the CRS Code of Conduct, the CRSs can continue to ignore them with impunity, and will have no financial incentive to spend money on compliance.

Enforcement has been, and remains, urgently needed to bring the CRSs into compliance with data protection norms, to protect data subjects against longstanding, ongoing vulnerabilities, and to enable CRS users to comply with their own obligations.

Some of the continuing threats caused by the lack of passwords for PNR access were publicly demonstrated in December 2016, exploiting some of the vulnerabilities I had written about publicly and brought to the attention of Amadeus, Sabre, and the predecessors of Travelport fifteen years earlier, beginning in 2001.[12]

In the absence of support by the CRSs for password controls on PNR access, numerous public-facing systems that rely on CRSs for data storage and functionality, including self-service check-in and itinerary viewing systems operated by airlines and travel agencies (or operated by CRSs in the names of airlines or travel agencies), rely on inherently insecure, fixed, CRS-assigned "record locators" in place of passwords. These record locators are printed on boarding passes, baggage tags, and itineraries. Travellers are never told that they need to treat record locators as unchangeable passwords.

---

10 See written Parliamentary question submitted to the Commission in 2011: "Has the Commission designated a point of contact or established procedures for handling complaints from individuals of violations of the Code of Conduct for CRSs? If so, how has the Commission made public this point of contact and the procedures for handling such complaints?" <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT+WQ+E-2011-011250+0+DOC+XML+V0%2F%2FEN&language=EN>. The answer to this question from the Commission did not mention the Code of Conduct, complaints, or any point of contact or procedures.

11 "European Commission to investigate airline reservation (in)security", <https://hasbrouck.org/blog/archives/002296.html=>

12 See links to video, slides, news reports, and commentary about the public demonstration, and my earlier reports of these vulnerabilities, at "Travel data: fraud with booking codes is too easy", <https://hasbrouck.org/blog/archives/002279.html >

Airlines accept this lack of security because it facilitates automation through self-service systems that reduce airline labor costs. More secure systems that require a unique or user-selectable password for access to each PNR would require more airline and/or airport staff to deal with lost or forgotten passwords, and might reduce or slow adoption of self-service check-in, flight change, or other labor-saving systems. In the absence of data protection enforcement, airlines have a financial interest in prioritizing their own business process automation over the security of travellers' personal data.

Airlines and other CRS users will implement more secure, but more costly, PNR access controls only if they are forced to do so through enforcement of data protection requirements, or if passwords are implemented by CRSs as requirements for all users.

Access logs are the other key missing piece, along with passwords, in the lack of CRS data protection. Access logs are an essential prerequisite for accountability or oversight of disclosures or transfers of personal data to other entities or countries.

Amadeus, for example, says that, "Due to the global nature of the travel industry, personal data may be transferred to and processed by Amadeus GDS Users in different locations around the world. These transfers will be necessary for the performance of a contract between the traveler and the Amadeus GDS User."[13] Similar claims are made by the other GDSs. But there is no basis for the claim that international transfers of CRS data are restricted to those that are "necessary".

In fact, anyone authorized by either an airline participating in the itinerary, a travel agency or tour operator that made the booking, or the CRS itself, in any of their offices or remote locations anywhere in the world (including in countries with no privacy or data protection laws), can access a PNR for any purpose. CRSs have not implemented any technical measures to enforce geographic or purpose limitations on access to PNRs, or to log access. There is no requirement for a CRS user to specify a purpose for access to a PNR, and no record of access is kept in the PNR.

In the absence of access logs or geographic or purpose limitations on access to PNRs, traveller profiles, or other data, the CRS has no record of which users have accessed personal data, which countries data has been transferred to, or for what purposes. Any response to a request by a data subject for an accounting of disclosures is necessarily pure speculation.

Until CRSs add immutable access logs to PNR histories, it will be impossible for any CRS user to provide an accurate or complete accounting of disclosures and international transfers of personal data contained in CRS records, or to comply with the privacy and data protection norms.

I would be happy to discuss this submission with you by phone, and/or to meet with staff of DG-MOVE or other concerned E.U. institutions on my next visit to Brussels.

13 "Privacy notice for Amadeus global distribution system ('Amadeus GDS')", <https://amadeus.com/en/policies/gds-privacy-statement>

I authorize public disclosure of this submission, including my name and contact information.

Sincerely,

Edward Hasbrouck
San Francisco, CA, USA
10 December 2018