THE PRACTICAL NOMAD

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

The Practical Nomad: How to Travel Around the World (4th ed. 2007)
The Practical Nomad Guide to the Online Travel Marketplace (2001)
http://www.practicalnomad.com

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

30 October 2009

Privacy Roundtables – Comment, Project No. P095416

Topic recommendations and request to participate as panelist: Federal Trade Commission "Public Roundtables on Consumer Privacy"

As an expert in travel records, I request that you include the category of travel data as a topic for your forthcoming series of "Public Roundtables on Consumer Privacy", and I request an opportunity to participate as a panelist to discuss the privacy issues posed by travel data. I could be available either in Washington on 7 December 2009, or at a West Coast roundtable.

1. The privacy problems of travel data

Personally identifiable information about consumers collected in relation to their reservation, purchase, and use of transportation and travel services is one of the the largest, most sensitive, most intimately revealing, most systematically computerized, most widely dispersed, most globally accessible, and most potentially subject to abuse categories of consumer data.

But unlike other categories of consumer data recognized as having special characteristics that warrant special protections and special regulatory attention, there is no sector-specific privacy legislation applicable to travel data in the USA, and this global problem has largely fallen through the jurisdictional cracks between multiple Federal, state, and foreign agencies.

Repositories and processors of travel data, centered around the small number of "Computerized Reservations Systems" (CRS's) or "Global Distribution Systems" (GDS's),[1] commingle data collected from multiple sources worldwide under multiple privacy jurisdictions.

1 See the discussion and list of the major CRS's/GDS's in my article, "What's in a Passenger Name Record (PNR)?", at http://hasbrouck.org/articles/PNR.html#CRS. Today these companies generally refer to themselves as GDS's, but were regulated in the USA under the label of "CRS's", and are still regulated in the EU as "CRS's".

A single "Passenger Name Record" (PNR)[2] stored in a CRS/GDS can and routinely does contain a mix of data collected by and/or under the direction of multiple governments, regulated common carriers, and ordinary commercial entities in multiple countries.

The global CRS/GDS and travel IT ecosystem exemplifies "cloud computing": It's often difficult, sometimes impossible, to determine who "owns" particular items of data in these records, or where in the world the servers that hold it are located.

CRS's/GDS's and the PNR's and customer profiles stored in them are used seamlessly by multiple parties, worldwide, for multiple purposes: by travel agencies as their outsourced customer relationship management, transaction, and accounting databases; by travel services providers as their operational databases for the delivery of travel services and for marketing; and by governments as sources of backward-looking "travel history" data (for profiling, social network analysis, etc.) and forward-looking "vetting" of would-be travellers.

Both as created by travel companies and as imported into US and other government records or accessed by governments, PNR's and other travel records contain extraordinarily intimate data. PNR's show where you went, when, with whom, for how long, and at whose expense. Behind the closed doors of your hotel room, with a specific person (identified, perhaps, by name, address, gender, data of birth, citizenship, passport or ID number, and credit card number) they show whether you asked for one bed or two.[3]

Of course, travel records are *per se* records of the exercise of protected rights. They record how, when, where, why, with whom, by what means, at whose expense, etc., we exercise the Federal statutory right to travel on interstate and international common carriers (who are required, as Federally regulated common carriers, to transport all passengers paying the fare and complying with the standard conditions in their published tariff), how we exercise the "right … to assemble" protected by the First Amendment to the Constitution, and how we exercise the freedom of movement guaranteed by Article 12 of the International Covenant on Civil and Political Rights (as ratified by and binding on the USA and as given effect through statutory provisions including those clauses of the Airline Deregulation Act requiring airlines to be licensed as common carriers and requiring Federal aviation regulators to consider in any rulemaking – as they have often failed to do, unfortunately – "the public right of transit"). [4]

PNR's and other reservation and travel records – both for common carriers and for hotels and other travel services – also contain billing, discount, and special service codes that reveal health and medical information, including information about invisible physical disabilities; confidential business information including insider information about business deals, alliances, and supplier and customer relationships; information about attorney-client relationships; information about associations and organizational affiliations, including labor union and political organization membership; and other types of especially sensitive and privileged information.

---

2 See my article, "What's in a Passenger Name Record (PNR)?", at http://hasbrouck.org/articles/PNR.html.

3 This is not a hypothetical. I have seen such bed type/number codes in copies of PNR's obtained from the DHS Customs and Border Protection "Automated Targeting System" in response to FOIA and/or Privacy Act requests.

4 See "Comments of the Identity Project et al., USCBP-2005-0003, Passenger Manifests for Commercial Aircraft Arriving in and Departing From the United States" (12 October 2006), available at http://hasbrouck.org/IDP/IDP-APIS-comments.pdf, and "Comments of the Identity Project, TSA-2007-38572, Secure Flight Program" (22 October 2007), available at http://hasbrouck.org/IDP/IDP-SecureFlight-comments.pdf.

Travel records are vulnerable to malign use by stalkers and other would-be perpetrators of domestic violence, by travel and other commercial entities for nonconsensual and privacy-invasive marketing, by authoritarian governments for surveillance and control of movements, and for industrial espionage by commercial competitors of business travellers.

Travel records are highly vulnerable to unauthorized access. Tens of thousands of travel agencies and airline staff in the USA alone, and many times more around the world, have credentials as authorized users of CRS's/GDS's. In many cases, those credentials permit remote login and access to CRS/GDS records via the Internet. Because no logs are normally kept of access to PNR's or customer profiles stored in a CRS/GDS, compromise of a travel agency's credentials, and unauthorized access using those credentials, could go undetected indefinitely.

CRS's/GDS's have deployed insecure public Web gateways that allow anyone who knows your name and "record locator" to view the complete itinerary from your PNR.[5] But a "record locator" is not a password and does not provide adequate access control: record locators are printed and displayed everywhere from itineraries and tickets to boarding pass stubs (frequently discarded after a flight) and the tags on checked luggage, which are exposed to public scrutiny, unattended, while on the carousel at the destination waiting to be claimed.

Because airlines, their general sales agents, and travel agencies in many countries are state-owned or parastatal entities, there is no meaningful distinction between what data stored in a CRS/GDS is accessible to travel companies that subscribe to those CRS's/GDS's, and what data is accessible to governments worldwide, including potentially unfriendly governments and governments that compete with (or share data with commercial competitors of) US businesses.

Most personally identifiable data in reservations and other travel records is not provided directly to service providers by consumers, but is either provided through intermediaries (travel agencies, operators of Web sites, etc.) or is entered by third parties without consumers' knowledge (e.g. free-text remarks and notes, sometimes personal and/or derogatory, entered in reservations by front-line travel agency and travel services provider staff).[6]

It's difficult for consumers to determine whether, in requesting or collecting or processing particular data, a given entity is acting on behalf of a government or governments, as a common carrier, as an agent of a common carrier, as a third-party contractor or service provider or intermediary, on its own behalf, or in some combination of multiple roles with respect to some or all of the same data. It's especially difficult for consumers to tell what rules are supposed to apply when data is collected by a commercial entity, but under color of a claim – which the consumer is, in most cases, unable to verify – that its provision is mandated by some government.

Multiple non-synchronous copies of travel records are routinely created in the ordinary course of business, and routinely persist long after the events they record are complete. This data is routinely accessible, worldwide, including by commercial entities and foreign governments, without consumers' knowledge or consent. Consumers typically aren't told, and cannot verify even if they try, what entities actually store these records, or where. The principal travel data

5 See my article, "Who's watching you while you travel?", at http://hasbrouck.org/articles/watching.html.

6 See the personal data flow diagram from my presentation at the Computers, Freedom, and Privacy Conference (3 April 2003) at http://hasbrouck.org/cfp2003/CAPPS2.html and the CRS cloud architecture diagram from the same presentation at http://hasbrouck.org/cfp2003/airarch.html . The CAPPS-II and the ASSR databases have both been renamed "Secure Flight", but the diagrams remain otherwise valid with those label substitutions.

warehouses and aggregators, including the CRS's/GDS's and other intermediaries[7], are invisible to consumers, have no direct dealings with them, and acknowledge no responsibility to them.

Many of the travel companies that deal directly with consumers, such as the major online travel agencies, routinely violate their stated privacy policies that claim to allow consumers to control how their data is used. I know of no major online travel agency that allows consumers to determine to which CRS's/GDS's or other processors, contractors, or intermediaries their personal information will be transmitted, or what the consumer privacy policies (if any) are of those CRS's/GDS's and other companies. Yet in their privacy policies, online travel agencies disclaim responsibility for the actions of those to whom they pass on information about consumers, and hypocritically advise consumers to consult the privacy policies of those (unknown and unknowable) third parties prior to making reservations or purchases.

It's equally difficult for consumers to tell whether personal data solicited in the course of a commercial travel reservation or purchase is optional or required; whether it is "required" purely as a business decision, as a condition of carriage on a common carrier, or by government mandate; whether (and if so, by whom) it will be used for operational, marketing, security, and/or surveillance purposes; and where, by whom, and for how long it will be retained.

Typically, no records are kept of where travel data was collected, what jurisdiction it is subject to, or by whom or from where in the world it has been accessed. Typically, in the USA, travelers and other individuals have no right to see what information is being kept about them, even when it is being made available to third parties and governments worldwide, and used by governments – in the USA and abroad – as the basis for decisions affecting their ability to exercise fundamental rights protected by statutes, the Constitution, and international treaty law.

The absence of access logs in the major CRS's/GDS's makes it impossible for travel companies that use these systems to comply with the fundamental principles of fair information practices – or even, in many cases, their own claimed privacy policies. Since no access logs are kept or included in PNR's, travel companies themselves don't know who has accessed data they entered. As they have admitted in response to some of my requests, they don't know and thus can't tell consumers who has accessed data about them, which data, or from where in the world.[8]

Travel was the first major category of e-commerce and the only major one to predate the Internet.[9] Travel services remain among the highest dollar-value products or services routinely purchased online. Even offline transactions with "brick and mortar" travel agencies and travel services providers are frequently recorded (and globally accessible by both commercial and governmental entities) in CRS's/GDS's or other global travel data networks. But the problems discussed above are especially acute in travel e-commerce. It's impossible to have a meaningful discussion of consumer privacy and e-commerce without considering *travel* e-commerce.

Unfortunately, travel data has often been overlooked in general discussions of consumer data privacy, for a variety of structural and historical reasons. The global cloud of travel IT

---

7 For a survey of some of those other intermediaries, including the Airlines Reporting Corporation (ARC), Vistrio, and the division of Amadeus formerly known as Airline Automation, Inc., see my article, "FBI wants records from travel data aggregators" (28 September 2009), at http://www.papersplease.org/wp/2009/09/28/fbi-wants-records-from-travel-data-aggregators/, and the other articles linked from that article.

8 See my articles, "KLM claims it doesn't know what happens with passengers' data" (8 August 2007) at http://hasbrouck.org/blog/archives/001273.html, and "What does Air France do with reservation data?" (10 May 2009) at http://hasbrouck.org/blog/archives/001679.html.

9 See my book, "The Practical Nomad Guide to the Online Travel Marketplace" (Avalon Travel, 2001).

infrastructure and data dissemination developed long before the Internet and before almost any other industry had so computerized or globalized its databases of records about consumers. When these issues later began to arise in other industries, pre-existing travel industry systems and practices have usually been overlooked. And travel IT has largely been its own "parallel universe" with its own norms, protocols, and practices and only limited crossover of knowledge, expertise, or even awareness of its existence by those involved in other industry sectors.

Much of the technical documentation is proprietary to the CRS/GDS companies, and many of the technical experts have acquired their expertise under nondisclosure agreements. Most of those who do have adequate expertise are those employed within the travel industry by companies with an interest in the ignorance of government regulators and consumer advocates.

There also has been, and continues to be, a malign coincidence of interest between commercial entities interested in tracking consumers' travel, behavior, and activities in as much detail as possible, and retaining and using those records for marketing and other commercial purposes, and some government agencies both in the USA and in the world's worst police states interested in collecting or getting access to the same data, and using it for purposes of surveillance and control of the movements of citizens and foreign visitors alike. Both travel marketers and police have an interest in maximum data collection and minimum transparency, since individuals would not consent to many of these practices if they were aware of them.

Finally – and perhaps most importantly with respect to the forthcoming FTC public roundtables and the next concrete steps toward addressing these issues – there has been in the USA neither any one agency given a clear leading role in development of privacy policy and regulatory and enforcement strategy for travel data, nor a clear division of authority between agencies, nor any forum for interagency coordination of policy, practice, and jurisdiction over travel data collected, maintained, and used by this diversity of government and private entities.

The privacy of travel data and the policies regulating its collection, retention, access, use, dissemination, and destruction should be a high priority concern for multiple agencies, including the FTC, the Department of Transportation, the Department of Homeland Security (including both Customs and Border Protection for records of international travel and the Transportation Security Administration for records of domestic travel), the Federal Communications Commission (which would appear to have jurisdiction, although it does not appear to have exercised it, over CRS's/GDS's as operators of electronic communications services and/or remote computing services subject to the Wiretap Act and/or the Stored Communications Act),[10] state and local consumer protection agencies (who have jurisdiction over most travel services providers other than interstate common carriers), and the privacy and data protection authorities of other countries. To the extent that consumers are not adequately protected by existing law, this should also be a priority for Congress, state legislators, and the National Conference of Commissioners on Uniform State Laws. And although travel data has often been considered to be *sui generis*, and in some respects is (although not in quite the ways it is usually assumed to be), no general discussion of consumer data privacy practices or policies would be meaningful or complete without significant consideration of the particularities of travel records.

As I've tried to explain above, records related to many aspects of a trip are routinely stored in the same PNR's in the same CRS's/GDS's. These systems have been developed with the specific goal of allowing *seamlessly integrated* reservations, purchasing, itinerary display, and delivery of travel services – through a network of networks that links several hundred thousand business entities worldwide, from independent hotels to global airline "alliances". No record is

10 United States v. Mullins, 992 F. 2d 1472, 1478 (9th Circuit, 1993)

generally kept of the purpose for which particular items of information were collected or entered, the jurisdiction to which they are subject, or the conditions attached to their use.

In a single transaction, through a single Web site or at a single travel agency, paid for with a single check or credit card charge, a consumer routinely reserves and purchases, through a chain of multiple (unseen, typically unknown, and deliberately invisible) intermediaries, services provided by interstate common carriers subject to exclusive Federal jurisdiction exercised primarily by the DOT (under the preemption clause of the Airline Deregulation Act)[11]; services provided by a CRS/GDS as the operator of an electronic communications service and/or a remote computing service subject to FCC and FTC jurisdiction; services to be provided by hotels, tour operators, or other businesses subject to concurrent state, local, and FTC jurisdiction; and services to be provided by the online or offline travel agency itself, which typically but falsely claims in its terms of service to be acting "solely as an agent of the carrier" even while charging a service fee that makes it a dual agent with fiduciary responsibilities both to the carrier and the consumer, subject to the jurisdiction of both the DOT (in the travel agency's capacity as an agent of the carrier) and the FTC and state and local authorities (in its capacity as an agent of the consumer and to the extent that it also acts as a merchant and principal in its own right).

The foregoing is, of necessity, only a cursory summary of some of the most severe privacy issues posed by travel records, and some of their roots in the information ecology of the travel industry and the symbiosis between government and industry users of this data. But I trust that this is sufficient to give some sense of the severity of the problem, and the urgent need to include this topic in the agenda of the forthcoming FTC privacy roundtables.

I look forward to the opportunity to share my expertise with the Commission and its staff, and to work with you to craft a program of action – by the FTC and other government bodies – to address these exceptionally serious threats to consumers' privacy.

2. Consumers' expectations of privacy in travel data

In its request for comments, the FTC has asked what are the expectations of consumers with respect to personal information provided in the course of consumer transactions.

Sadly, we must distinguish consumers' expectations of what *will* happen from their expectations of what *should* happen. While most consumers are unaware of most of the uses and recipients of commercial data about their travels, they have come to expect – correctly, given the current lack of any US privacy law applicable to travel data, and the inability of foreign governments that do have such laws to enforce them against US companies including the US-based CRS's/GDS's that host and disseminate much of this data – that their travel data, like all of their consumer data, *will* be misused by government and industry alike.

At the same time, consumers continue to expect (1) that travel data about them *should* be treated as their data and their informational property, not the property of third parties to which it has been provided for specific and limited purposes, and (2) that when personal information is provided to a third party in a commercial context, the default legal assumption *should* be that is provided for a particular purpose, and that no grant of a license to use it for other purposes should be presumed.

---

11 For some of the problems with DOT jurisdiction and Federal preemption as they have been exercised, see my article, "Federal airline consumer protection agenda" (23 October 2009) at http://hasbrouck.org/blog/archives/001755.html, and the documents linked form that article.

Those expectations are, of course, routinely violated in the USA, with travel data as with other categories of personal information about consumers.

The issue of whether data about me is "my data", or is actually owned by commercial entities that have collected or obtained it, is most important when such a company goes bankrupt.

No consumer actually intends to agree, when they provide personal information to a business, that if the company goes bankrupt, that personal information not only can but should and must be sold to the highest bidder for the sole benefit of the company's creditors, not the individuals to whom that data pertains. In assuming this, the bankruptcy laws flagrantly violate any reasonable or likely understanding of consumers actual expectations.

The possibility of a bankruptcy auction of a personal data archive about consumers is not limited, of course, to the possibility of bankruptcy of a travel company. But there are few, if any, industries that combine the frequency of bankruptcies of even the largest companies with the volume and sensitivity of personal information and consumer profiles that are held by travel companies such as airlines and hotels. Airlines are routinely in and out of bankruptcy, and in the last year large numbers of hotel owners have gone bankrupt.[12]

Luckily, most recently bankrupt airlines have been reorganized or have had their assets including their data archives bought by other airlines. There is no guarantee that this luck will hold. It is only a matter of time before a major airline or hotel chain is a liquidated, and the bankruptcy court is required by current law to auction its records of years or decades of consumers' travels to the highest bidder. Based on discussions of this issue with travel database marketing professionals, I think it highly unlikely that in such an auction any other airline could match the bids of data brokers, data aggregators, data miners, and direct marketers.

Reform of the bankruptcy laws is *urgently* needed to protect personal information about consumers, which they provided to a particular company for a particular purpose, from being sold at bankruptcy auction to an unrelated third party, most likely a data mining or direct marketing company, without the consent of the individuals to whom this data pertains. And the potential bankruptcy liquidation of a travel company is clearly the paradigmatic case of the danger posed by the current lack of protection in bankruptcy law for personal information.

The counter-factual presumption of US law that (in the absence of any explicit contractual terms to the contrary) the consumer intends to grant an unrestricted and irrevocable license in perpetuity for any and all use of personal data is embodied in principles of contract interpretation that can probably best be addressed through revision of the Uniform Commercial Code. That is obviously beyond the authority of the FTC, but the FTC can and should work with the privacy community and state consumer protection agencies to craft proposals to the National Conference of Commissioners on Uniform State Laws to revise the UCC to incorporate more realistic default assumptions about the limits of the implied grant of rights to use of personal information.

3. Recommended actions for the FTC and its partners

No one agency has the jurisdiction or the expertise to address this issue completely alone. I strongly recommend the creation of a dedicated interagency working group or task force on travel data and privacy, including Federal, state, and foreign consumer, transportation, and

12 See my article, "FAQ about Airline Bankruptcies", at http://hasbrouck.org/articles/bankruptcy.html.

security agencies, charged with working closely with privacy and technical experts outside governments, including privacy advocates and independent experts as well as industry insiders.

Such a task force could, as a first step, clarify the jurisdictional boundaries between agencies, to ensure that there are no jurisdictional gaps and that policies and activities are coordinated and harmonized where jurisdiction overlaps. A particularly important place to start would be coordination of privacy related activities between the FTC and the Office of Aviation Enforcement and Proceedings of the Department of Transportation, particularly as that jurisdiction relates to travel agencies who act simultaneously and often in the same transaction as agents of common carriers, agents of consumers, and merchants and principals in their own right.

Such a task force could also address the question of personal information provided simultaneously to multiple parties for multiple purposes, or provided to one party for one purpose, but under current business practices and technology infrastructure made available to other entities at the same time. For example, DHS currently requires travellers to provide additional personal information including APIS[13] and Secure Flight[14] data to travel companies. But while that data is unneeded for any commercial purpose, and is provided only under DHS mandate for DHS purposes, travel companies have to date been allowed free and unrestricted use of this data for their own purposes, without any obligation of notice or consent. Travel companies and other commercial entities should be categorically forbidden from using data provided under government mandate for any other purpose without customer consent, and should be required to delete this data after it has served its government purpose.

Similar issues arise when personal information is provided as a condition of travel by common carrier, with the additional unresolved question of what, if any, personal information can lawfully be required (taking into consideration statutory, Constitutional, and international treaty provisions) as a condition of the exercise by common carrier of the right to travel.

FTC/DOT coordination is also required with respect to the privacy policies of common carriers. I believe that it is in all cases a fraudulent and deceptive business practice to advertise a privacy "policy" that is not explicitly incorporated into contractual terms. But even if the FTC does not adopt that position, there are particular issues regarding the enforceability of a privacy policy for a common carrier, if that privacy policy is not included in their published tariff. Common carriers are required to publish and abide by a tariff, and are forbidden to enforce any contractual terms not specified in that tariff. Common carriers should not only be required to include privacy policies meeting defined standards in their tariffs, but should all so be subject to enforcement sanctions for fraud if they publish a purported privacy policy without filing it as part of the generally applicable terms and conditions in their tariff.

The FDC need not, however, wait for other agencies or for the establishment of an interagency task force on travel privacy to begin to address the problems I have raised. Some of these issues can be dealt with by the FTC on its own.

In particular, the FTC can and should tackle the privacy problems of CRS's/GDS's immediately.

---

13 See my article, "Permission to Travel" (15 October 2006), at http://hasbrouck.org/blog/archives/001156.html.

14 See "Secure Flight: Frequently Asked Questions" at http://www.papersplease.org/sf_faq.html, my article, "Public hearing in Washington on "Secure Flight" (13 September 2007) at http://hasbrouck.org/blog/archives/001286.html, and my testimony at the TSA hearing on Secure Flight (20 September 2007) at http://hasbrouck.org/articles/SecureFlight-20SEP2007.pdf.

The major CRS's/GDS's were all originally developed as in-house projects of airlines, and as such were subject to DOT jurisdiction. For many years they were also subject to orders promulgated by the Department of Justice under its antitrust authority. But the DOJ regulations have been withdrawn, and the three major US-based CRS's/GDS's are no longer airline owned.[15]

While the FTC does not yet appear to have noticed, jurisdiction and responsibility for privacy protection for consumer travel data held by CRS's/GDS's has now passed to the FTC. The FTC should not hesitate to address this urgent need, and to propose new legislation if necessary. CRS's/GDS's have an even more central and significant role for travel data than do credit bureaus for consumer financial data. Since almost all other travel companies depend on CRS's/GDS's as outsourced connectivity, infrastructure, and in many cases database hosting providers, CRS/GDS functionality defines the *de facto* limits of potential travel privacy.

Unless CRS/GDS operators add access logging, more granular access controls including geographic and purpose limitations, and the capability to track permissions for particular items of data (not just for an entire PNR and all the melange of data it contains) it will be impossible for even the best-intentioned of other travel companies to comply with the principles of fair information practices. (Travel agencies already have a near-impossible task, since they act as agents for hundreds of airlines based in other countries around the world, and are obligated when executing contracts to which those airlines are the principals to observe the laws of their home jurisdictions.) But CRS's/GDS's are unlikely to make the necessary investment in these infrastructure changes and upgrades to functionality unless compelled to do so. Access logging by CRS's/GDS's, in particular, should be mandated by the FTC as soon as possible.

As a matter of policy, it is just as important for consumers to know what is in their travel records – which are accessible to the DHS and government agencies abroad in real time, even when they are held by CRS's/GDS's or other commercial entities, and which are used to make decisions about whether to permit individuals to travel – as it is important for them to know what is in their credit reports. FTC regulations or legislation mandating that CRS's/GDS's allow consumers access to their travel records could and should be adopted as soon as possible, starting from the model provided by the Fair Credit Reporting Act and access rules for financial data warehouses and aggregators.

These are just some of the obvious first steps, but would be significant ones.

4. Background and expertise

Edward Hasbrouck[16] is a leading expert on the content, usage, potential for malign usage, infrastructure, and technical and policy issues posed by commercial travel records, particularly "Passenger Name Records" (PNR's) used to store airline, hotel, car rental, tour, cruise, and other travel reservations and purchase records, as well as the "Computerized Reservation Systems" (CRS's) or "Global Distribution Systems" (GDS's) used to store PNR's and other records and for communications within and between travel agencies and travel services providers.

Hasbrouck is the author of "The Practical Nomad: How to Travel Around the World" (4th edition 2007, Avalon Travel) and "The Practical Nomad Guide to the Online Travel Marketplace"

15 For an overview of the history and rationale for CRS/GDS regulation in the USA, Canada, and EU, as well as my recommendations for CRS/GDS privacy rules, see my article, "Europe reconsidering rules for reservation systems" (4 March 2007) at http://hasbrouck.org/blog/archives/001225.html.

16 Bio: http://hasbrouck.org/bio/. Disclosures and disclaimers: http://hasbrouck.org/disclosures.html (These comments are offered solely on my own behalf, and not on behalf of my publisher, past employers, consulting clients, or any organization including those of which I am a member)

(Avalon Travel, 2001), and articles on his Web site and blog at http://www.hasbrouck.org including “What's in a Passenger Name Record (PNR)?” and other FAQ's about privacy and other consumer issues for travelers. He is also a regular contributor on travel privacy to the Identity Project Web site and blog at http://www.papersplease.org.

Hasbrouck won a Lowell Thomas Travel Journalism award in 2003 from the Society of American Travel Writers Foundation for his self-published online investigative reporting on the privacy of travel records, and has contributed articles on travel data and privacy to *Privacy Journal* and Privacy International's *Privacy and Human Rights* yearbook. He has testified on travel privacy issues before the Transportation Security Administration, the Data Privacy Advisory Committee of the Department of Homeland Security, and the California state legislature, and has provided declarations as an expert witness on travel reservations technology, data content, and business practices in public interest and consumer litigation against government agencies and travel companies in the USA and Canada. He has participated in meetings with members and staff of Congress, the European Parliament, the European Commission, the European Data Protection Supervisor, and the Article 29 Working Party of European Union national data protection authorities, and has attended and reported on workshops on travel document and data standards conducted by the International Civil Aviation Organization.

As a consultant for the Identity Project (PapersPlease.org), a nonprofit educational and advocacy organization, Hasbrouck has provided technical and policy analysis and comments on the implications for privacy, civil liberties, and human rights of numerous regulatory proposals by the Department of Homeland Security, Department of State, and other agencies. As an individual consumer advocate, he has provided comments on Department of Transportation proposals related to enforcement of consumer protection rules for travel companies.

Hasbrouck's background includes more than 15 years of travel industry experience, including extensive technical experience with CRS/GDS and PNR formats, operations, and interfaces, managing CRS/GDS conversions, and participation as CRS/GDS data format and usage subject-matter expert in development of customized and proprietary CRS/GDS interface, integration, and business process automation software for an online travel agency.

Hasbrouck's blog, The Practical Nomad”, at http://www.hasbrouck.org/blog/, has been recognized and recommended by the *New York Times*, the *Times* (UK), and the *Wall Street Journal* as one of the leading consumer and business travel blogs.

Hasbrouck has been featured in a BBC-TV travel documentary, spoken at National Geographic Society headquarters in Washington, and been quoted and interviewed as a consumer travel expert by CNN, CNBC, "Computer Chronicles" on PBS, "The Savvy Traveler" and "Marketplace" on NPR, Pacifica Radio, Voice of America, *The New York Times, London Sunday Times, Wall Street Journal, Los Angeles Times, Washington Post, Miami Herald, Christian Science Monitor, USA Today, Chicago Tribune,* AP, UPI, Reuters, *Newsweek, Business Week,* Wired News, Salon.com, CBS MarketWatch.com, FoxNews.com, TheStreet.com, Bankrate.com, *Aviation Week, TravelAge West, Travel Weekly, Airline Financial News, World Airline News, Business Travel News, Kiplinger's Personal Finance, National Geographic Traveler, National Geographic Adventure, Toronto Star, Detroit Free Press, Minneapolis Star-Tribune, Rocky Mountain News, Seattle Post-Intelligencer, Portland Oregonian, Kansas City Star,* and numerous other media outlets. In the San Francisco Bay Area, he's been seen on KGO and KRON television; heard on KPFA, KQED, KPOO, and KALW public radio; and quoted in the *San Francisco Chronicle, San Jose Mercury News, Oakland Tribune,* and *Contra Costa Times.*

Hasbrouck has spoken at travel industry, technology, and policy conferences including the Computers, Freedom, and Privacy conference and eTravelworld; events for travellers including Hostelling International "International Travel Days" in the USA and Independent Travellers' World in London; colleges and universities; associations, clubs, and civic forums including The Commonwealth Club, the Globetrotters' Club, the World Trade Club, and the Sierra Club; and at travel bookstores, hostels, and other venues in the USA, UK, and Canada.

Hasbrouck has gone around the world three times himself, once in each of the last three decades. His most recent trip, in 2007-2008, covered more than 80,000 miles over 13 months, visiting 28 countries on 6 continents. Hasbrouck has visited all 50 states of the USA, 8 Canadian provinces, and more than 50 other countries, travelling by foot, bicycle, train, bus, boat, car, taxi, rickshaw, donkey and pony cart, and on more than 50 different airlines.

Hasbrouck is a member of numerous professional associations, human rights groups, and travel consumer advocacy organizations including the Consumer Travel Alliance, the National Writers Union (Co-Chair, Book Division), the Bay Area Travel Writers (former member, Board of Directors), the Travel Website Owners Association, the National Lawyers Guild, Tourism Concern, Ethical Traveler, Hostelling International (life member), the National Association of Railroad Passengers, the Train Riders Association of California, the San Francisco Bicycle Coalition, and the National Lawyers Guild (non-lawyer legal worker member).

Respectfully submitted,

Edward Hasbrouck
edward@hasbrouck.org
+1-415-824-0214

San Francisco, CA
30 October 2009