Before the

FEDERAL TRADE COMMISSION

Washington, DC 20580

Advance Notice of Proposed Rulemaking (ANPR): **Trade Regulation Rule on Commercial Surveillance and Data Security** **R111004**	**COMMENTS OF** **EDWARD HASBROUCK**

Edward Hasbrouck
1130 Treat Ave.
San Francisco, CA 94110

telephone +1-415-824-0214
edward@hasbrouck.org
https://hasbrouck.org

August 30, 2022

By an Advance Notice of Proposed Rulemaking (ANPR) published on August 22, 2022, at 87 *Federal Register* 51273-51299 ("Trade Regulation Rule on Commercial Surveillance and Data Security, Advance notice of proposed rulemaking; request for public comment; public forum", R111004,) the Federal Trade Commission (FTC) has requested comments concerning "the prevalence of commercial surveillance and data security practices that harm consumers."

As a consumer and human rights advocate; an investigative journalist and winner of awards for reporting on commercial surveillance and data security practices; an invited expert witness on privacy issues related to airline reservation data at hearings before the Advisory Committee for Aviation Consumer Protection of the U.S. Department of Transportation, the Canadian House of Commons, and the the European Parliament; and an expert on the real-world harms to consumers of commercial surveillance and data (in)security practices, especially in travel-related industries; I welcome the opportunity to respond to this request for comments.[1]

My comments address two key questions in the ANPR:

"5. Are there some harms that consumers may not easily discern or identify? Which are they?"

"8. Which areas or kinds of harm, if any, has the Commission failed to address through its enforcement actions?"

My answers below to these questions highlight two unrecognized or under-appreciated issues that should be priorities for the FTC in its rulemaking and enforcement activities and its legislative recommendations to Congress: the inability of individuals to see what information has been collected about them ("subject access rights"), and gaps or uncertainties between Federal agencies with respect to the boundaries of regulatory and enforcement jurisdiction, particularly with respect to transportation and communications common carriers and their service providers.

I urge the FTC to prioritize, through rulemaking, enforcement, and if necessary legislative recommendations, (A) **subject access rights** and (B) **jurisdictional gaps and uncertainties** related to transportation and communications common carriers and their service providers – especially the computerized reservation systems or global distribution services that host extremely sensitive but currently poorly-secured airline and other travel reservation data.

"**5. Are there some harms that consumers may not easily discern or identify? Which are they?"**

In general, consumers cannot discern or identify the harms or risks of data collection and use, whether by government agencies or commercial entities (or both of these in collaboration),

1. See links to some of my writing on this topic at <https://hasbrouck.org/articles/travelprivacy.html>. I plan to testify at the public forum being organized by the FTC on September 8, 2022, in conjunction with this ANPR. However, given the two-minute time limit for testimony by each witness at the public forum, my verbal testimony will be only a brief summary of these written comments.

without being able to see, in comprehensible form, exactly what data is being collected about them by whom, and to what third parties which specific data has been disclosed ("shared").

For good reason, "subject access rights" are a core principle of fair information practices: "Individual Participation Principle: 13. Individuals should have the right… to have communicated to them, data relating to them… in a form that is readily intelligible to them."[2]

For good reason, neither a general description of the data nor a list of categories of data is sufficient to satisfy the OECD guidelines for subject access as a fair information practice.

Neither a general description of the data nor a list of categories of data is sufficient to enable individuals to assess the risks of activities or transactions about which data may be collected, to grant meaningfully informed consent, to make an informed choice of which data they may want to have deleted, or to effectively mitigate the damage in case of a data breach.

Time after time, I have seen that individuals are unable to appreciate the significance, harm, or risk of vaguely-described categories of data or recipients of data, unless and until they can see either their own data, in full, or a clearly-explained example of an actual full data set.

Businesses that collect, use, and "share" personal data can and will do their best, usually successfully, to describe data and recipients in terms that are vague, incomplete, and/or innocuous seeming, even when the actual data is highly sensitive and would not be consented to.

For example, as an expert with fifteen years of industry experience working with airline reservations and the companies that collect, use, and share reservation data, I have requested my own data from airlines and computerized reservation systems[3], posted templates on my Web sites members of the public to use to make such requests, and offered my services to assist individuals – including other privacy experts and journalists – in interpreting the responses. records

Time after time, people who told me that they didn't think there was anything sensitive in their airline reservations have discovered that there was data in those reservations – often cryptically coded – that they didn't know was included and wouldn't have consented to, but that, without expert assistance in interpreting the responses, they would not have recognized the meaning of. Indeed, I can't recall a single instance in which I have reviewed an individual's passenger name record (PNR) data[4] without finding some data they were surprised by, and/or finding that the response was obviously (to me as an expert reviewing the complete response) incomplete in some way that would not be apparent to an ordinary consumer, and would give them the false impression of having received a full and (misleadingly) reassuring disclosure.

2. OECD, "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.
3. U.S. law provides no subject access rights to this data from airlines or CRSs, but laws in Canada and the European Union provide subject access rights to data collected by or transferred to Canadian or EU airlines.
4. See my explainer, "What's in a Passenger Name Record (PNR)?", <https://hasbrouck.org/articles/PNR.html>.

Subject access rights are sometimes wrongly perceived as secondary to other aspects of data privacy. But in practice, subject access rights and access logs accessible to data subjects are an essential *prerequisite* to informed consent to collection or disclosure of personal information, or to any meaningful ability to assess threats or mitigate damages from data breaches.

I urge the FTC to recognize that individuals cannot truly "consent" to data collection or disclosure unless they can actually see and understand what data has been collected or disclosed. In the absence of explicit consent to collect information while keeping it secret form the person to whom it pertains, refusal to disclose specific personal data should be deemed conclusive evidence that the individual has not, and could not have, consented to its collection or disclosure.

Businesses may argue that few individuals will actually exercise their right to inspect the data that those businesses hold about them. This is probably true, but is not a reason not to provide subject access rights to those who wish to exercise them. It may take only a few well-explained examples to show individuals what is contained in a particular data set. But without subject access rights, no such examples will be available to consumers at all.

Internal "privacy officers" typically review privacy *policies* rather than *practices* for compliance with privacy principles. Only through the exercise of subject access rights can either consumers or independent watchdogs audit whether businesses practice what they preach.

Subject access rights are also, as *should* be obvious, especially important in the event of a data breach. One of the first things an individual should do – and should be entitled by law to do – in the event of a suspected or actual data breach is to obtain and review a complete copy of the data pertaining to them held by the entity that was, or might have been, breached.

A general description or list of categories of breached data is insufficient to enable individuals to take appropriate or effective action to mitigate the damage from a data breach.

A notice that "credit card information" has been compromised is useless for threat assessment or damage mitigation without knowing which information about which credit card has been compromised. How else can a consumer know which card(s) they need to cancel?

For example, a little over a year ago information about tens of millions of current and former customers of T-Mobile USA was breached. I'm one of those T-Mobile customers. When I was notified – which wasn't until two months later – that personal information about me had been compromised, the data was described in only the vaguest terms, such as "drivers license/ID information", without any further details.[5] Was this information about some ID I had when I became a T-Mobile subscriber in 2004? Or one of the IDs I have today? Which ID (my passport? my drivers license? some other ID?) was compromised? And what information from that ID (ID number? validity dates? photograph? signature?) did T-Mobile have? I still don't know.

5. See data breach notice at <https://hasbrouck.org/documents/T-Mobile/T-Mobile-notice-26OCT2021.pdf> .

More than a year after the T-Mobile data breach, despite diligent efforts, I still have been provided with access to *none* of the data about me that was breached. T-Mobile adamantly refuses to provide any of the specific pieces of information that I have requested, and T-Mobile's controlling owner, Deutsche Telekom, refuses to compel T-Mobile to do so.[6]

The purportedly "complete" response from T-Mobile to my subject access request contains none of the specific pieces of information that were breached and that I have requested, only vague and unhelpful generalities that raise more questions than they answer.[7] What "olfactory information" does T-Mobile collect, for example, and why? I have no idea.

So far as I can tell, no customer of T-Mobile or any other major U.S. mobile communications network operator has been allowed to see all the data the company collects about them, including location tracking logs – even when I and other customers have specifically requested this data about ourselves. Like many companies, T-Mobile records customer service calls, but refuses to allow customers access to these recordings of their own calls.

Few consumers object or withdraw "consent" for these practices, *because* none of them have seen what data is being collected. Many would object if they saw what data is collected. When Deutsche Telekom, in response to a lawsuit in Germany, responded to just one subject access request for location data, and that customer was able to visualize and show the public this data,[8] it led to consumer pressure for changes in the company's data retention practices.

It's characteristic of the deprecation of subject access rights relative to other principles of fair information practices that, although T-Mobile's actions are in flagrant violation of the California Consumer Privacy Act (CCPA), the CCPA creates a private right of action for certain data breaches but not for violations of subject access rights. So T-Mobile's denial of subject access rights, which continues to frustrate the ability of tens of millions of current and former T-Mobile customers such as myself to assess the threat and mitigate the damage from the breach of our data, are not addressed in the proposed settlement of class-action lawsuits against T-Mobile.[9]

"8. Which areas or kinds of harm, if any, has the Commission failed to address through its enforcement actions?"

In addition to violations of subject access rights and rights to an accounting of disclosures (where those rights are recognized by U.S. law, which in many instances they aren't), the FTC and other agencies including the Department of Transportation (DOT) and the Federal Communications Commission (FCC) have failed – as a result of gaps or uncertainties as to the

6. See, "T-Mobile and Deutsche Telekom lie to customers", August 9, 2022, <https://hasbrouck.org/blog/archives/002653.html >
7. See unredacted (although both incomplete and mostly unintelligible) response at <https://hasbrouck.org/documents/T-Mobile/T-Mobile-Personal-Information-Access-Report.pdf>.
8. Kai Biermann, "Betrayed by our own data", Zeit March 10, 2011, https://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz >, and TED Talk by Malte Spitz, "Your phone company is watching", <https://www.ted.com/talks/malte_spitz_your_phone_company_is_watching>.
9. See details of proposed settlement at <https://www.t-mobilesettlement.com/>.

boundaries of their respective jurisdictions – to adequately address harms from privacy and security violations committed by transportation and communications common carriers and by businesses that host data and provide other information technology services to common carriers.

These failures have been pointed out repeatedly over many years, but persist.

The jurisdictional problems and potential gaps between the FTC and FCC with respect to *communications* common carriers were noted and described in an FTC staff in a report last year.[10]

But significant as these problems are, the privacy issues and jurisdictional problems between the FTC and the DOT over *transportation* common carriers are even more severe.

As an expert in the privacy implications of travel data, it is my firm opinion, founded on decades of experience, that information about the movements of our *physical bodies* – the information obtained, used, and too often disclosed by transportation companies – is, in general, more sensitive and subject to more damaging potential misuse than the information about the movements of our *messages* obtained, used, and disclosed by communications companies.

While location data held by communications companies, including cellphone location data, shows where we have been, travel reservations show also where we plan to go in the future, when, and with whom. Computerized reservation systems have information not only about the trips we took and plan to take, but the trips we thought about and canceled, or are considering but haven't committed to. It's because of these attributes as a uniquely revealing source of almost "mind reading" predictive information about our intentions and plans for the future that information obtained from travel reservation companies under statutory mandate[11] or court order[12] is such a priority target for acquisition by government surveillance agencies around the world.

These problems with respect to the privacy of travel data are greatly exacerbated by the fact that most transportation carriers, especially airlines, like many other travel companies, outsource hosting of their reservation databases to third-party computerized reservation systems (CRSs) or global distribution systems (GDSs).

When a CRS or GDS hosts reservation data on behalf of an airline, do the preemption provisions of the Airline Deregulation Act apply to the activities and personal data handling practices of that CRS/GDS? Does jurisdiction lie with the FTC, the DOT, both – or neither?

---

10. "A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers", FTC Staff Report, October 21, 2021 <https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf >.
11. See the Identity Project, "How airline reservations are used to target illegal searches", September 17, 2013, <https://papersplease.org/wp/2013/09/17/how-airline-reservations-are-used-to-target-illegal-searches/>.
12. See the Identity Project, "Sabre and Travelport help the government spy on air travelers", July 1, 2022, <https://papersplease.org/wp/2022/07/01/sabre-and-travelport-help-the-government-spy-on-air-travelers/>.

Do the FTC and DOT have an agreement and common understanding of the boundaries of their respective jurisdictions that insures that nothing falls through the gaps? Or are there areas over which neither agency exercises meaningful oversight, because each agency thinks the other agency has (or might claim) exclusive or primary jurisdiction?

And if exclusive jurisdiction lies with the DOT, does the DOT have adequate subject-matter expertise, given that the DOT has no history of enforcement related to data privacy?

Given the lack of any history of enforcement with respect to this category of data, the uncertainty and/or hesitancy by either the FTC or DOT to asset jurisdiction, and the apparent lack of subject-matter expertise or privacy enforcement resources on the part of the DOT, it should be no surprise that transportation carriers and the CRS/GDS companies that host reservation data have lagged behind other industries in their privacy and data security practices.

Stalkers, identity thieves, or other attackers can retrieve PNR data with only a "record locator" that has none of the attributes of a secure password. I wrote about this vulnerability more than twenty years ago,[13] and it has been publicly demonstrated.[14] Nothing has been done about it, presumably because airlines and CRS/GDS companies see no threat of enforcement.

PNR data is accessible worldwide, without access logs or purpose limitations, so most breaches are undetectable unless the perpetrators are caught in the act of confess. Changes would have to be made by the CRS/GDS companies before it would even be possible for an airline to provide an accounting of disclosures of reservation data

Both the privacy problems of travel data and the problems caused by the division of privacy jurisdiction between the FTC and the DOT were discussed in comments I submitted to the 2009 FTC Privacy Roundtables in conjunction with the Consumer Travel Alliance, Consumer Federation of America, and Center for Financial Privacy and Human Rights.[15]

So far as I can tell, no action has been taken by the FTC, DOT, or Congress with respect to any of the problems or any of the recommendations for action in those comments.

These issues and recommendations were also raised when I was invited to testify at the before the DOT Advisory Committee for Aviation Consumer Protection (ACACP) in May 2013,[16] (the first time any DOT body held any public discussion of the privacy issues with travel

13. Edward Hasbrouck, "Who's watching you while you travel?", April 20, 2002, <https://hasbrouck.org/articles/watching.html>.
14. Edward Hasbrouck, "Travel data: fraud with booking codes is too easy", December 27, 2016, <https://hasbrouck.org/blog/archives/002279.html>.
15. Comments of Edward Hasbrouck, CTA, CFA, and CFPHR, "Privacy Roundtables – Project No. P095416", November 6, 2009, available at <https://hasbrouck.org/articles/Hasbrouck_et_al-FTC-6NOV2009.pdf>.
16. See Edward Hasbrouck, slides summarizing testimony and recommendations, "Consumer Privacy and Air Travel: Recommendations to the U.S. Department of Transportation, Advisory Committee for Aviation Consumer Protection", May 21, 2013, <https://hasbrouck.org/articles/Hasbrouck-ACACP-21MAY2013.pdf>.

data) and in a joint letter to the ACACP from myself and fifteen other privacy, consumer advocacy, and civil liberties organizations and experts in December 2013.[17] These submissions have also gone unheeded, while the problems they highlighted persist and continue to grow.

While the Wiretap Act and other Federal statutes create some sector-specific protections for communications data, there is still no sector-specific Federal legislation creating any protections whatsoever for travel data. Travel data, including data collected by or on behalf of Federally-licensed transportation common carriers, remains *by far* the most sensitive category of consumer data, with the greatest potential for abuse or for harm if breached, that is not yet subject to any sector-specific Federal privacy guarantees.

The CRSs and GDS – companies entirely unknown to most consumers, but which hold a treasure trove of extraordinarily intimate data (behind the closed doors of your hotel room with this other person, named and identified by age and gender, did you ask for one bed or two?) have, across the board, some of the worst privacy and data insecurity norms of any industry.

As such, travel data including common-carrier and CRS/GDS data should be among the highest priorities for the FTC's exercise of its general enforcement and regulatory authority, for coordination with other agencies including the DOT to avoid jurisdictional gaps or misunderstandings, and for Congressional action if needed to close jurisdictional gaps.

I thank the FTC for taking the initiative to address this important issue. I would be happy to discuss these comments and potential follow-up actions with FTC members and/or staff.

Respectfully submitted,

/s/

Edward Hasbrouck
1130 Treat Ave.
San Francisco, CA 94110

telephone +1-415-824-0214
edward@hasbrouck.org
https://www.hasbrouck.org

17. Joint letter to the Department of Transportation, Advisory Committee for Aviation Consumer Protection (ACACP) from the Consumer Travel Alliance, Consumer Federation of America, Privacy Rights Clearinghouse, Privacy Times, Consumer Action, Privacy Activism, Electronic Privacy Information Center, National Network to End Domestic Violence, Center for Financial Privacy and Human Rights, National Workrights Institute, World Privacy Forum, American Civil Liberties Union, Edward Hasbrouck, Remar Sutton, Robert Ellis Smith, and Kathryn A. Serkes, December 2, 2013, <https://hasbrouck.org/articles/privacy-ACACP-DEC2013.pdf >.