AMERICAN UNIVERSITY
WASHINGTON, DC

Statement of
Jennifer Daskal

Associate Professor
American University Washington College of Law

Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection
United States House of Representatives

Hearing on
21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies Impact on U.S. Jobs

October 12, 2017

WASHINGTON COLLEGE OF LAW
4300 NEBRASKA AVENUE, NW WASHINGTON, DC 20016
http://www.wcl.american.edu

Statement of
Jennifer Daskal
Associate Professor
American University Washington College of Law

Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection
United States House of Representatives

Hearing on
21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies Impact on U.S. Jobs

October 12, 2017

Chairman Latta, Ranking Member Schakowsky, and Members of the Committee, thank you for inviting me to testify.

The free movement of data across borders is critical to economic growth, has benefits for data security, and promotes privacy, speech, and associational rights. Yet, increasingly states are adopting a range of measures that restrict data flows to the United States and elsewhere and adopting costly data localization mandates, pursuant to which companies must store data locally.[1] Such restrictions on the free movement of data harm U.S. business interests, undermine the growth potential of the Internet and thus the global economy, and undercut both data security and privacy.

International data flows increased world GDP by 10 percent compared to a world without such flows, according to a recent McKinsey report.[2] The benefits for the United States are particularly strong. The U.S. International Trade Commission reports that digital trade—loosely defined as economic activity involving Internet technology and the cross-border movement of data—increased U.S. GDP by 3.4-4.8 percent in 2011, resulting in a significant increase in wages.[3] Restrictions on the free flow of data threaten this important source of economic growth.

Data security is also put at risk when service providers are forced to store all data on local servers, rather than distribute the data across different storage sites in multiple

[1] *See, e.g.,* Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L. J. 677 (2015) (detailing a range of localization mandates); ALBRIGHT STONEBRIDGE GROUP, DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION (Sept. 2015), http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf.

[2] See JAMES MANYIKA, SUSAN LUND, JACQUES BUGHIN, JONATHAN WOETZEL, KALIN STAMENOV, & DHRUV DHINGRA, DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS, MCKINSEY GLOBAL INSTITUTE, (Feb. 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

[3] U.S. INT'L TRADE COMMISSION, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, Part 2 13 (Aug. 2014), https://www.usitc.gov/publications/332/pub4485.pdf.

locations.[4] Localization mandates also can result in business being shifted from major online providers to smaller local equivalents. This too can create additional security risks. Smaller, local providers often have weaker security protections than major multinational companies with the resources to respond to increasingly sophisticated cyber thieves.[5]

Moreover, whereas data localization mandates are often described as a means of protecting privacy, they often have the converse effect. They provide a means for repressive regimes to keep tabs on citizens and residents in ways that can stifle dissent—or worse.

Such restrictions on the free flow of data are often directed specifically at the United States or adopted in direct response to concerns about U.S. policies and market power. The motivating factors are multiple—including fears about the scope of U.S. foreign intelligence surveillance, concerns about the adequacy of U.S. consumer privacy protections, a desire by foreign governments to ensure their own ability to access sought-after data, and sheer protectionism. There is, as a result, no single, all-encompassing solution. But there are nonetheless important steps that the United States can take to address some of the motivating forces and thereby promote a free and open Internet.

In what follows, I suggest four areas of reform designed to address each of the key concerns motivating such restrictions.

1. Surveillance Reform

Concerns about the reach of U.S. foreign intelligence surveillance have led foreign governments and foreign-based customers to seek out non-U.S.-based companies to manage their data and to insist on data localization—with significant costs to the U.S. tech industry.[6] In 2015, the European Court of Justice (ECJ) sent shock waves through the business community in the United States and Europe by striking down the then-in-place Safe Harbor Framework, largely due to concerns about U.S. intelligence surveillance in the wake of the Snowden revelations.[7] The Safe Harbor Framework had been relied on by well over 4,000 companies as a means of assuring (via a self-certification process) that they had "adequate" privacy protections in place as required by EU law, and thereby permitting the transfer of personal data from the EU to the United States.

---

[4] *See* DANIEL CASTRO, THE FALSE PROMISE OF DATA NATIONALISM 1 (Info. Tech. & Innovation Found., Dec. 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf ("The notion that data must be stored domestically to ensure that it remains secure and private is false").

[5] *See* Chander & Le, *supra* note 1, at 719.

[6] *See, e.g.*, Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies,* N.Y. TIMES, Mar. 21, 2014; DANIEL CASTRO & ALAN MCMCQUINN, BEYOND THE USA FREEDOM ACT: HOW U.S. SURVEILLANCE STILL SUBVERTS U.S. COMPETITIVENESS (Info. Tech. & Innovation Found., June 2015) https://www.scribd.com/embeds/268099469/content?start_page=1&view_mode=scroll&show_recommendations=true (asserting that concerns over U.S. surveillance practices in wake of the Snowden revelation are likely to cost the U.S. tech sector more than $35 billion).

[7] *See* Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, 2015 E.C.R., ¶ 94-95, http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN.

The subsequently negotiated Privacy Shield Framework is currently relied on by approximately 2,500 companies as a basis for engaging in the cross-continental transfer of personal data.[8] A range of companies also rely on what are known as standard contractual clauses, which offer an alternative means of establishing the legality of such transfers.[9] But both Privacy Shield and standard contractual clauses are subject to legal challenge as well—based on ongoing concerns about the reach of U.S. surveillance.[10] In fact, just two weeks ago, the Irish High Court concluded that there are "well founded concerns" about the adequacy of the privacy protections provided for by standard contractual clauses. The Irish Court focused on the reach of U.S. foreign intelligence surveillance and the perceived absence of effective remedies.[11] The case has now been referred to the ECJ.[12]

Meanwhile, several Members of the European Parliament also have expressed concerns about both the scope of U.S. surveillance and the absence of sufficient accountability mechanisms for EU citizens.[13] An expert group of European privacy officials have raised concern about bulk surveillance by the United States and the failure to staff the Privacy and Civil Liberties Board (PCLOB), which provides important oversight of U.S. surveillance policies and practices.[14] An ECJ ruling or broader policy determination that U.S. legal protections are inadequate to support cross-continental transfers of personal data would be devastating to the free flow of data from the EU to the U.S. and to U.S. businesses.

Some of the EU's critiques reflect a mischaracterization of U.S. policies and practices and elide key changes to US surveillance policies and practices over the past several years. These include the passage of the Judicial Redress Act, which extends protections of the Privacy Act of 1974 to the citizens of the EU and other designated foreign countries;[15] the passage of USA Freedom Act, which put an end to the government's bulk collection of domestic telephony metadata, requires declassification reviews of significant Foreign Intelligence Surveillance Court (FISC) opinions, and

---

[8] *See* Sam Schechner, *Europe's Top Court to Review Privacy,* WALL ST. J. (Oct. 4, 2017).

[9] Other possible mechanisms for supporting the cross-continental transfer of personal data include consent by the data subject (although the standard for finding valid consent can be hard to meet); binding corporate rules (although these only permit intra-corporation transfers and do not allow transfers to unaffiliated entities, such as customers and suppliers); and reliance on approved codes or conduct. *See* Lothar Determan, Brian Hengesbaugh & Michaela Weigl, *The E.U.-U.S Privacy Shield Versus Other EU Data Transfer Compliance Options*, BLOOMBERG BNA (Sept. 12, 2016) (detailing various transfer options).

[10] *See* Case T-670/16, Dig. Rights Ireland v Comm'n, 2016 O.J. (C 410) 26; Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems (Schrems II), [2017] 2016 No. 4809 P (H. Ct) (Ir.) (Oct. 3, 2017), https://iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf (referring case to ECJ).

[11] Schrems II, [2017] 2016 No. 4809 P at ¶ 334.

[12] *Id.*

[13] *See* European Parliament resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield, (2016/3018(RSP)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0131+0+DOC+PDF+V0//EN.

[14] See Article 29 Data Protection Working Party, Press Release, *Preparation of the Privacy Shield annual Joint Review* (13 June 2017).

[15] Judicial Redress Act of 2015, Pub. Law No. 114-126 (2016).

mandates enhanced transparency about Foreign Intelligence Surveillance Act (FISA) collection;[16] and adoption of new executive branch guidance designed to better protect the privacy interests of foreigners.[17]

But ongoing concerns about the perceived overreach of U.S. foreign intelligence collection and the sufficiency of accountability mechanisms loom large, and there is more that Congress can do to assure the EU and other key allies that their concerns are being taken into account. Specifically, Congress can and should push for the following key reforms. Together, they will help assure foreign governments that the United States adequately protects the privacy interests of their citizens and residents and thereby better protect the free flow of data from the EU and elsewhere.

First, with section 702 of the Foreign Intelligence Surveillance Act of 2008 set to sunset this December, Congress should take this opportunity to implement additional protections designed to better safeguard privacy, consistent with the government's intelligence needs.[18] Among other reforms, Congress should codify the end to the collection of "about" communications—something the executive branch has already put a stop to as a matter of policy.[19] As the terminology suggests, an "about" communication contains a reference to (is "about") an email or phone number associated with a particular target, rather than being directly to or from the target's email or phone number. It thus sweeps in a significant amount of incidental collection on those that would not otherwise be deemed legitimate, direct targets of such collection.

Notably, the House Judiciary Committee's recently released USA Liberty Act includes an eight-year prohibition on "about" collection; this is something that should be widely supported.[20] Other provisions of the USA Liberty Act require enhanced reporting and accountability measures, mandate the appointment of amicus curiae to the FISC to assist in the issuance of 702 certifications, and put in place improvements to the Privacy and Civil Liberties Oversight Board (discussed in more detail below); these too deserve wide support.[21] Such reforms would help to ensure the EU and other foreign governments that U.S. surveillance programs are subject to enhanced accountability

---

[16] USA FREEDOM Act of 2015, Pub. Law No. 114-23 (2015).

[17] *See* WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE—SIGNALS INTELLIGENCE ACTIVITIES § 4 (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD-28].

[18] The 702 program authorizes the National Security Agency to, pursuant to Foreign Intelligence Surveillance Court approval of minimization and targeting procedures, acquire the communications of foreigners located outside the United States for the purposes of gathering foreign intelligence information. For a detailed analysis of the program. For an excellent overview of the 702 program, *see* PRIVACY & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014), http://www.pclob.gov /library/702-Report.pdf.

[19] *See* Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets*, N.Y. TIMES (April 28, 2017).

[20] H.R. 3989, 115th Cong. § 102(a)(2) (2017).

[21] Additional reforms, some of which are also included in the USA Liberty Act, are also needed to protect the Fourth Amendment interests of U.S. persons, including limits on FBI searches of the databases for U.S. person information. Here, however, I am focused on reforms that would provide protections for U.S. persons and foreigners alike, consistent with the goal of promoting the free flow of data.

mechanisms and thus help preserve the free flow of data.[22]

Second, Congress should mandate what Presidential Policy Directive 28 (PPD-28) does as a matter of policy. PPD-28 was issued by President Obama in response, in large part, to foreign government concern about the scope of US surveillance and applies to all signals intelligence activity (not just that covered by 702). Specifically, Congress should codify the requirement that "signals intelligence activities . . . include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides." Congress should also codify the presumption (taken from PPD-28) that protections for personal information collected through signals intelligence apply to U.S. citizen and foreign data alike: "To the maximum extent feasible consistent with the national security, these policies and procedures [designed to safeguard personal information] are to be applied equally to the personal information of all persons, regardless of nationality."[23]

Third Congress should work with the administration to reinvigorate and put in place improvements to the Privacy and Civil Liberties Oversight Board (PCLOB). Created in 2007 and first operational in May 2013, the PCLOB provides oversight over foreign intelligence collection so as to ensure that such actions are balanced with the need to protect privacy and civil liberties. The PCLOB's reports on both the telephony metadata program and the 702 collection programs have been highly influential—providing some of the most extensive information about these programs and ultimately contributing to the dismantling of the bulk collection of telephony metadata.[24] Of particular importance, the PCLOB has been designated as the review body for complaints referred by the Privacy Shield ombudsman, a position set up in the wake of Privacy Shield to receive and review complaints regarding national security access to data transferred from the EU to the US

Now down to one board member, the PCLOB lacks a sufficient quorum (three out of the five members) to continue to function. In an encouraging sign, the administration has recently nominated a new PCLOB Chair. Congress should move quickly to hold hearings on the nomination, push for the nominations of other board members, and reinvigorate this critically important oversight body. The PCLOB's continued operation is something that can help ensure the continued vitality of Privacy Shield.

In addition, Congress should adopt the provisions included in the bipartisan USA Liberty Act that ensure the board can carry out key functions even during a period of vacancy by the Chair and permit board members to engage in informal discussions without being subject to the requirements of the Sunshine Act. Meanwhile, the

[22] H.R. 3989, *supra* note 20 §§ 103, 104, 107, 201- 203.
[23] PPD-28, *supra* note 17, at § 5.
[24] *See* REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, *supra* note 18; REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 (Jan. 23, 2014), https://www.pclob.gov/library/215-report_on_the_telephone_records_program.pdf.

provisions requiring that the Board hold public hearings, inform the public of its activities, make its reports public to the greatest extent possible should be kept intact.[25]

2. Consumer Privacy Protection

This summer's breach at Experian—pursuant to which the personal and confidential information of nearly half of the American's population was exposed—highlights once again the need for better consumer privacy protections in U.S. law. Enhanced consumer privacy requirements are things that any company doing business in Europe will already be familiar with—given the requirements of EU's soon to be implemented General Data Protection Regulation (GDPR). The GDPR, which will go into effect in May 2018, applies to all companies that process the personal data of EU data subjects, regardless of the company's location and mandates an array of protections for consumer privacy.[26] Enhanced consumer privacy protections will also help ensure the future of Privacy Shield—protecting it from legal and policy-related challenges.

In other words, strengthening consumer privacy protections is not only good policy, but something that just about any company that wants to do business in the EU is going to have to implement anyway, will help ensure the future of Privacy Shield, and will help to disincentivize protectionist policies based on a claimed need to protect consumer privacy.

I suggest three key reforms.

First, Congress should pass a strong data breach notification statute. This should set a minimal floor, putting in place strict obligations for timely and rolling notification, while also permitting states to innovate and demand more.[27] Pursuant to the GDPR, timely notification is something that companies doing business in Europe will already be required to do; breach notification to authorities is generally required within 72 hours, and notification to affected data subjects "without undue delay" in specified circumstances.[28] The fact that Equifax took some six weeks and perhaps longer to notify its customers about the breach should remind Congress of the need for legislative action in this area.

Second, Congress should enact a Privacy Act for the private sector—what has often been called a Consumer Bill of Rights.[29] Whereas the Privacy Act grants

---

[25] See 42 U.S.C. 2000ee(f); ADAM KLEIN, MICHELE FLOURNOY, AND RICHARD FONTAINE, SURVEILLANCE POLICY: A PRAGMATIC AGENDA FOR 2017 AND BEYOND 39 (Dec. 2017) (recommending that PCLOB be exempted from the Sunshine Act), https://www.cnas.org/publications/reports/surveillance-policy.

[26] Regulation (EU) 2016/679 of 27 April, 2016, General Data Protection Regulation, 2016 O.J. (L 119) [hereinafter GDPR].

[27] *See, e.g.,* Danielle Citron, *The Privacy Policymaking of State Attorney General*, 92 NOTRE DAME L. REV. 747, 767-769 (2016) (describing data breach notification requirements being mandated by states).

[28] GDPR, *supra* note 26, arts 32-34.

[29] *See Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows: J. Hearing Before the U.S. H.R. Energy & Commerce Subcomms. on Commerce, Mfg., and Trade and Commc'ns and*

individuals a tool to learn about it and correct mistakes with respect to personal data in the hands of the federal government, there are no equivalent protections vis-à-vis the private sector. Congress should rectify this. It should ensure that individual consumers are provided a statutory basis to protect their own personal data and correct mistakes made and potentially promulgated by the private sector. And it should oblige the private sector to take reasonable steps to protect data security, coupled with the creation a private right of action.

Third, the Federal Trade Commission (FTC) should be given the authority to impose financial penalties for privacy and security violations, even the first time there is a compliance problem, and to impose larger fines than is currently possible. Currently, the FTC is not permitted to impose financial penalties on most first time offenders. These changes would help better incentivize companies to protect consumer security and privacy.[30]

3. Law Enforcement Access

Provisions of the Electronic Communications Privacy Act (ECPA) are imposing hard-to-justify barriers on foreign governments' ability to access communications content, such as emails, critical to their own investigations of serious crime—simply because the data happens to be U.S.-held. This is true even if the foreign government is investigating its own national in connection with a local crime and the *only* U.S. nexus to the data is that it happens to be held by a U.S.-based company in the United States. Instead, the foreign government is required to go through the mutual legal assistance process and initiate a diplomatic request for the data.

Consider, for example, U.K. law enforcement investigating a London murder spree. The U.K. officials seek the data of the alleged perpetrator in order to help establish motive. If the perpetrator uses a U.K -based provider, the officials could access the data within days if not sooner. But if instead he uses a U.S.-based service provider, the U.K. officials are told that they must make a request for the data through the U.S. government, employing the mutual legal assistance treaty (MLAT) process—a laborious and time-consuming process that generally takes multiple months, sometimes years.[31]

Tech., 114 Cong. 1 (2015) (testimony of Marc Rotenberg, President, Electronic Privacy Information Center) (calling for the adoption of a Consumer Bill of Rights).

[30] See Tara Siegel Bernard & Stacy Cowley, *Equifax is Facing Scrutiny. If Only it had Come a Bit Sooner,* N.Y. TIMES (Sep. 9, 2017) (noting that just last month, for example, the FTC punished TaxSlayer, a tax preparation service, yet lacked the authority to issue any fines because it was a first-time compliance action); Daniel J. Solove & Woody Hartzog, *The FTC and the New Common Law of* Privacy*,* 114 COLUM. L. REV. 583 (2014) (providing an excellent and thorough account of the privacy jurisprudence of the FTC).

[31] *See, e.g.*, RICHARD A. CLARKE ET AL., PRESIDENT'S REV. GRP. ON INTELLIGENCE & COMMC'N TECH., LIBERTY AND SECURITY IN A CHANGING WORLD 226-29 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (noting that the United States takes an average of ten months to respond to official requests made through the MLAT process for email records).

Foreign governments are understandably frustrated. And they are being incentivized to support data localization requirements in response—thereby ensuring access to sought-after data without having to go through the MLAT process.

Draft legislation sent to the Hill initially by the Obama administration and then again by the Trump administration would begin to address this problem. The legislation would amend ECPA so that foreign governments can, in specified and narrow circumstances, directly compel the production of communications content from U.S.-based providers, so long as baseline substantive and procedural protections are in place. This kind of direct access would only be available to those countries that entered into executive agreements with the United States; would continue to require use of the mutual legal assistance process if the foreign government were accessing the data of U.S. citizen or legal permanent resident or anyone located in the United States; and would require reciprocal rights of access to the United States in cases where it is seeking foreign-held data.

Moreover, the legislation includes a number of specific criteria designed to protect privacy and civil liberties. Among other requirements, the requests would have to be particularized, targeted, based on articulable and credible facts, and subject to judicial review or oversight; non-relevant information must be segregated, sealed, and deleted; and protections must be in place to ensure that the requests are not used as a means of acquiring information about a U.S. citizen or resident. There is room for some of these requirements could be strengthened, but in general they provide a notable set of baseline protections.

The criteria are sufficiently stringent that, at least initially, only a handful of countries would likely meet the requirements necessary to enter into the kind of executive agreements envisioned. As a result, it will not be a total panacea to the law enforcement-related concerns that are incentivizing data localization mandates around the globe. Nor should it be understood as such. But it would help disincentive data localization efforts with those countries with which the United States entered into the requisite executive agreements. And over time, it would establish a model—and baseline standards—that could be adopted more widely. It is legislation that Congress should, with some modest improvements, move quickly to adopt.[32]

4. Protectionism and Free Trade

The United States can and should make the maintenance of a free and open Internet, pursuant to which data flows freely across borders, a centerpiece of its trade agenda. Here, I focus on three key efforts that the United States should pursue in this

[32] *See also Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: S. Judiciary Comm.* (2017) (testimony of Jennifer Daskal, Professor, American University Washington College of Law), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Daskal%20Testimony.pdf (describing draft legislation in more detail); Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security & Rights Issues,* 8 J. NAT'L SECURITY L. & POL'Y 473 (2016).

regard.

First, the United States should leverage trade agreements to both eliminate and prevent barriers to data flows across borders. The now-defunct Trans-Pacific Partnership, for example, included a set of provisions would have prohibited mandatory data localization requirements. Similar and even stronger provisions should be included in other trade agreements as well.

Second, Congress should push the executive branch to continue to track digital protectionism and forcefully advocate the free flow of data in its bilateral and multilateral interactions, separate and apart from the treaty process. The placement of so-called digital trade officers in a handful of U.S. embassies is a start; this type of digital diplomacy should be expanded and encouraged.

Third, Congress should also push the administration to, when appropriate and preferable as part of a multilateral effort, initiate actions against those countries that are violating free trade obligations. More specifically, it should work to establish the important principle that data localization requirements violate free trade principles.[33]

Conclusion

The free flow of data is good for privacy, security, and economic growth both domestically and globally. Yet, countries around the world are implementing a range of policies designed to restrict the free flow of data—in many instances pointing to U.S. policies and practices as a justification for doing so. Stemming this trend will require a multi-pronged strategy designed to address the privacy and security concerns expressed by foreign governments while also taking steps to stem the protectionist impulses that contribute to these trends. Doing so will be good for the economy, good for security, and good for privacy—both domestically and globally.

[33] *See* Nigel Corey, *Cross-Border Data Flows: Where are the Barriers, and What Do they Cost?*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION 13-17 (May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.65050406.927448598.1504895329-310094596.1504895329 (making similar and additional recommendations).