CENTER FOR
DIGITAL
DEMOCRACY

5 July 2017

Bruno Gencarelli
Head of Unit
Directorate-General Justice and Consumers
European Commission
Via Email

Dear Mr. Gencarelli:

The Center for Digital Democracy (CDD), a leading U.S. NGO specializing in consumer data protection issues in the digital marketplace, is pleased to respond to the request that we provide information applicable to first annual review of the EU-US Privacy Shield. CDD has been assessing the Privacy Shield since it came into force in 2016, in part as a result of its work coordinating the activities from the U.S. side of the Transatlantic Consumer Dialogue (TACD) working group on the Information Society.

EU citizens and consumers who deal with companies enrolled in the Privacy Shield program confront a serious erosion of their data protection and privacy rights. The rights of EU citizens under the Privacy Shield program are not equivalent to how they would be protected by EU law. We urge the Commission and EU Data Protection Authorities to suspend the Privacy Shield in light of its lack of any policies, rules, or enforcement that would provide meaningful adequacy or equivalency. The Commission should insist that U.S. companies targeting EU citizens or consumers must operate under the forthcoming General Data Protection Regulation (GDPR) framework.

For this submission, we reviewed the activities of several major U.S. companies enrolled in the Privacy Shield program, examining their submissions on the U.S. Commerce Department website (including descriptions of their activities, the link to and content of their privacy policy statements). We compared these statements to the actual data collection and use-related activities conducted by the companies, including their own descriptions of how they operationalize their business goals. We supplemented this analysis with the information that CDD extensively gathers on the commercial digital marketplace, such as automated “programmatic” decision-making and other contemporary consumer-directed applications.

Our findings are as follows:

1. **There is no effective legal framework to protect consumer privacy in the U.S., with inadequate enforcement of the weak policies in place and an overall failure to address the dramatic growth of data practices**.
   Moreover, there is political opposition from the Congress and the White House to having effective data-protection rules. Perhaps the most evident sign that the U.S. cannot be considered as having equivalency or adequacy is the March 2017 decision by the Congress and President Trump to overturn the only major consumer privacy regulation enacted in decades to address the consumer digital marketplace. The Broadband Consumer Privacy Rules, adopted by the Federal Communications Commission in October 2016, would for the first time have provided the American public with actual protections and rights when their data are gathered and used in the marketplace. The new policy was widely supported by nearly every leading consumer and privacy NGO in the U.S., as well as many others who are concerned about the lack of data-protection policies in the U.S.[1] Not since the Congressional passage of the Children's Online Privacy Protection Act in 1998 had the U.S. enacted a rule promoting consumer privacy online. While primarily impacting Internet Service Providers (ISPs), specifically the cable and telephone companies that bring both wireline and wireless broadband connections and services to the public, the rule would have created important protections related to the overall U.S. data-gathering system (including tracking, profiling, programmatic targeting, sensitive data and more). ISPs and leading trade groups representing the most powerful U.S. data companies (such as Google and Facebook) worked to kill this new data-protection rule precisely because it put the U.S. on a path to begin improving its own legal framework for addressing consumer privacy.[2] Unlike the FTC, the FCC has the authority to issue regulations to protect the public, including for privacy. In March, President Trump signed the bill that overturned the only chance Americans had to see some improvement in how their data are collected.[3] While industry lobbyists and supporters of killing the FCC privacy rule claimed that it wasn't necessary because of the work of the Federal Trade Commission, such an argument was a sad joke on the American public. The industry knows, as does anyone who follows the U.S. data-gathering system, that the FTC does not have any meaningful rulemaking authority to regulate privacy (with the exception of COPPA, a law that CDD was largely responsible for enacting).

   Even before the Trump administration, the FTC has been incapable of effectively addressing how to empower and protect consumer digital privacy.[4] Many of the problems that the EU public now faces regarding how companies gather and use their information can be tied to the failure of the FTC to respond to what has been an alarming loss of privacy. Over the last four or so years, U.S. digital marketing companies have been able to expand—without limit—their use of programmatic,

"real-time" ad targeting on all platforms; identify, track, and target individuals regardless of their device; harvest an array of consumers' geolocation information, including their actual location and overall geographic behaviors; access an ever-growing abundance of information for consumer profiling made readily available from the explosion of so-called marketing or data "clouds"; work with dozens of partners that provide extensive access to other data sources; instantly add so-called "first-party" personal data with other information that can be readily uploaded to leading digital targeting sites; engage in sophisticated multichannel campaigns that create powerful new ways to access consumer data through social, video, native, mobile and other digital ad applications; take full advantage of individuals' (including adolescents') personal and sensitive information, such as their race, ethnicity, health status and age; and undermine the privacy of individuals and groups through the process called "look-alike" modeling, where a person's profile helps target others without their awareness at all. All of these practices have been exported and applied to the EU market by companies enrolled in the Privacy Shield—because they set the global baseline for how the digital ad market operates—and have been implemented by EU-based companies as well.[5]

The FTC has made no attempt to address these practices that undermine privacy, because the agency does not have the regulatory ability to do so. It has long called on Congress to give it rulemaking capability, something that the U.S. data lobby has successfully opposed. In addition, there are unfortunate historical reasons why the FTC is fearful of forcefully representing the public when it comes to consumer protection in the media marketplace.[6]

2. **The Privacy Shield principles permit far-reaching data use practices that operate on an ineffective "Notice and Choice" framework. Key EU data policies, such as on purpose limitation, sensitive data, are ignored.**
For example, we reviewed the Privacy Shield submissions of Axciom, including for its "data onboarding" subsidiary LiveRamp. An EU consumer would never know by reading its generally vague "Purpose of Data Collection" description on the Privacy Shield site that, for example, "LiveRamp Identity Link is an identity resolution service that ties data back to real people and makes it possible to onboard that data for people-based marketing initiatives across digital channels"; or that marketers use Axciom's LiveRamp to "create an omnichannel view of consumers…recognize consumers across touchpoints…tie media exposure to purchase data"; or that LiveRamp has far-reaching data partnerships with data brokers, digital ad companies, and the like; or that companies can use Axciom to conduct such data-targeting operations involving "audience suppression," "look-alike modeling," and "online to offline attribution."[7]

Adobe, another Privacy Shield enrollee, fails to explain its actual role facilitating the ever-growing collection and use of a consumer's data via its multitude of marketing

cloud applications, including, for example, that its "Adobe Audience Manager helps you build unique audience profiles that you can use anywhere — web, social, search, and mobile. It lets you combine first-, second-, and third-party data in one place so you can get a complete view of individual customers… making it possible to identify and target your most valuable segments on any platform."[8]

Similarly, one has to ignore what programmatic ad-tech company and Privacy Shield participant DataXU says on its Commerce Department submission, and review instead the much more revealing material it makes available to clients and prospective clients on its own website. There, one finds, for example, a recent "Forrester Wave" report that shows how DataXu specializes in "cross-device mapping, allowing marketers to import and export proprietary data and device graphs in and out of the DSP…. DataXu also allows marketers to customize machine learning with an algorithm marketplace and the ability to 'bring your own data.'"[9] In addition, it's clear that DataXu enables targeting consumers via the use of "online and offline data, media data, CRM data, First-and third party data, Web data and Private second-party data."[10]

EU citizens rightly believe that their geographic and place-based privacy should be protected. But another Privacy Shield enrollee—Factual—helps target them "based on…real world behavior" involving their mobile devices. They would not know that Factual's "Observation Graph combines location data and sensor data from mobile devices with Factual's digital understanding of the world to create discrete "observations on mobile users." This includes surveillance of "Place based behavior including visitation to specific places, merchants, and chains; Event attendance including concerts, sports, arts and more; Activity detection including driving and walking; User-specific places such as home and work, and Digital activity including apps used and device characteristics." Factual also promises that "New types of observations can be added as more data becomes available."[11]

Finally, while CDD also reviewed several other Privacy Shield participants, including MediaMath (which engages in "audience scoring," among other problematic practices), and The Trade Desk (which offers "geofencing: reach users based on real-time latitude/longitude location with hyperlocal geotargeting"), we also want to highlight the role of leading advertising agencies that have developed extensive holdings of data and the means to use that information for targeting.[12] Omnicom, for example, also a Privacy Shield member, operates a "powerful Insights Platform to squeeze every drop of value out of your most coveted data sources…in any format, at any time, processing 2 billion rows of data in 30 seconds…." Like other ad agencies, Omnicom operates divisions that specialize in data acquisition and use.[13]

3. **Self-Certification is both inadequate and dangerous as a means of protecting the EU public.** The Commission should have required the Department of Commerce and

the FTC to first "vet" the applications of Privacy Shield seekers through a review of their actual data practices. The DPAs should also be more vigilant. Self-certification has allowed U.S. companies to operate their data collection practices in the EU without regard to the meaning and spirit of the Directive, let alone the forthcoming GDPR. If the Commission had required the Department of Commerce and FTC to review the applicants, it would have quickly discovered there isn't the ability—or the will—to ensure that EU data rights are protected.

4. **The Privacy Shield website and submissions have numerous problems, reflecting overall disregard for its operations and impact on the public.** Submissions by Privacy Shield applicants are full of typos, broken links, and sloppy data entry.[14] The website itself is not designed to be user friendly in terms of its search functions. It suggests that no one at the Commerce Department or the FTC ever actually reviews what is being posted and the claims that are made.

In light of these findings, CDD calls on the Commission to terminate the Privacy Shield agreement and to call on the U.S. to enact privacy rules that meaningfully reflect the principles and policies of the forthcoming GDPR. Companies participating under the "cover" of the Privacy Shield are able to use programmatic and other automated and data-driven decision-making and practices that effect EU citizens' and consumers' ability to obtain financial services, health information, and buy products and services fairly. The failure of the U.S. to have its own effective legal privacy framework, the lack of oversight and enforcement by the Commerce Department and the FCC, and the failure of Privacy Shield participants not only to disclose their practices but also to ensure that they fully respect the EU approach to data protection, are among the reasons why the Commission must act now to protect the public.

The TACD will be raising these issues at a public forum in Washington, DC, this coming October, including the need for companies serving the EU market to implement the GDPR provisions in the U.S. as well.

Respectfully,

Jeffrey Chester
Executive Director
Center for Digital Democracy
1875 K Street, NW
4th Floor
Washington, DC 20006

[1] https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules/wheeler-statement; https://www.nytimes.com/2016/10/28/technology/fcc-tightens-privacy-rules-for-broadband-providers.html; https://consumersunion.org/news/consumers-union-praises-final-fcc-broadband-privacy-rules/

[2] https://arstechnica.com/tech-policy/2017/02/isps-wont-have-to-follow-privacy-rules-if-gop-lawmakers-get-their-way/; https://www.ncta.com/news-and-events/media-room/content/statement-ncta-internet-television-association-; https://www.iab.com/news/fcc-stay-broadband-privacy-rules/regarding-us-senate-approval-cra-regarding;

[3] http://www.politico.com/tipsheets/morning-tech/2017/04/trump-makes-it-official-and-signs-broadband-privacy-cra-219590; http://www.businessinsider.com/trump-fcc-privacy-rules-repeal-explained-2017-4; http://www.consumerreports.org/privacy/trump-signs-resolution-killing-fcc-internet-privacy-rules/

[4] https://www.mediapost.com/publications/article/272060/ftcs-ohlhausen-criticizes-broadband-privacy-propo.html; http://adage.com/article/privacy-and-regulation/ftc-chair-history-opposing-stricter-privacy-rules/307704/

[5] See for example, https://www.iab.com/guidelines/programmatic-rtb/; https://www.placed.com/targeting; https://www.oracle.com/marketingcloud/products/data-management-platform/index.html; https://adexchanger.com/advertiser/top-ten-programmatic-advertisers/; https://www.thinkwithgoogle.com/marketing-resources/programmatic/programmatic-native-advertising-mobile/; http://www.mediamath.com/audience/partner-audiences/; https://www.thetradedesk.com/partners; https://martechtoday.com/report-data-onboarding-important-marketers-192924; https://www.lotame.com/1st-party-2nd-party-3rd-party-data-what-does-it-all-mean/; https://www.facebook.com/business/a/us-hispanic-affinity-audience; https://www.thinkwithgoogle.com/interactive-report/gen-z-a-look-inside-its-mobile-first-mindset/; http://www.audiencepartners.com/healthcare-case-study-4/. To see some of these practices implemented in the EU: https://www.exchangewire.com/. We also note that political and electoral information may be being transferred, such as through Cambridge Analytica's Privacy Shield status: https://www.privacyshield.gov/participant?id=a2zt00000008PdqAAE&status=Active; https://commercial.production.i.cambridgeanalytica.org/privacypolicy

[6] https://iapp.org/news/a/ftc-commissioners-call-for-more-authority-federal-breach-law/; https://www.clickz.com/ad-industry-fights-to-stop-stronger-ftc-and-wins-for-now/55489/. See also the discussion of the "kidvid" episode decades ago that led to Congress removing FTC regulatory powers: http://www.fdalawblog.net/fda_law_blog_hyman_phelps/2011/10/kidvid-flashbacks-ftc-considers-curtailing-proposed-voluntary-principles-for-marketing-food-to-child.html

[7] https://www.privacyshield.gov/participant?id=a2zt0000000TNnVAAW&status=Active; https://www.acxiom.com/what-we-do/liveramp-identitylink/; https://liveramp.com/partners/;https://liveramp.com/partner/krux/; https://liveramp.com/applying-identitylink/for-brands/

[8] https://www.privacyshield.gov/participant?id=a2zt0000000TNo9AAG&status=Active; http://www.adobe.com/privacy/policy.html; http://www.adobe.com/privacy/marketing-cloud.html; http://www.adobe.com/marketing-cloud.html; http://www.adobe.com/experience-cloud/use-cases/customer-intelligence.html?promoid=KVGRV77V&mv=other

[9] https://info.dataxu.com/rs/275-QML-501/images/DataXu_Forrester_DSP_Wave_Q2_2017.pdf?mkt_tok=eyJpIjoiTTJOaE56STBZVGRtTkdNMiIsInQiOiJlTXpOaHc1djVRXC8xV01OT0kzSXFKdTAzNWpsdXIrTSs4VVkxclBSbWt6QUUzbWEwNzhwRk5LOWVmVSttaVp4M1BkSzErbnc0OThCWWtSenJTbmpmb0RzckFyWm5CK2I3MUJZditYb0thS3JINkJ4RlBuV1QzMEMzdGNDdFJoOSsifQ%3D%3D. This report also discusses Adobe and other Privacy Shield participants as well.

[10] https://www.privacyshield.gov/participant?id=a2zt0000000CbQiAAK&status=Active; https://www.dataxu.com/data-management/#interactions-across-devices; https://www.dataxu.com/data-management/#data-integration;

[11] https://www.privacyshield.gov/participant?id=a2zt0000000TNnfAAG&status=Active; https://www.factual.com/products/geopulse-audience; https://www.factual.com/technology/ads/observation-graph

[12] https://www.privacyshield.gov/participant?id=a2zt0000000TNxpAAG&status=Active; http://www.mediamath.com/privacy-policy/; http://www.mediamath.com/audience/audience-scoring/; http://www.mediamath.com/audience/lookalike-audiences/; https://www.privacyshield.gov/participant?id=a2zt0000000TNT1AAO&status=Active; https://www.thetradedesk.com/general/privacy-policy#background; https://www.thetradedesk.com; https://www.thetradedesk.com/products/data-management-platform-dmp

[13] https://www.privacyshield.gov/participant?id=a2zt000000000reAAA&status=Active#industries; http://www.omnicomgroup.com/privacy-notice/; https://www.annalect.com/technology/; https://adexchanger.com/agencies/annalect-contributed-omnicoms-big-year/; https://www.hearts-science.com

[14] See, for example, https://www.acxiom.com/about-us/privacy/eea-transfers-to-usa/; https://www.privacyshield.gov/participant?id=a2zt0000000TNxpAAG&status=Active; https://www.privacyshield.gov/participant?id=a2zt0000000TNT1AAO&status=Active