EXHIBIT 2

Alan Friel (SBN 166177)
afriel@bakerlaw.com
Blythe Kochsiek (SBN 285389)
bkochsiek@bakerlaw.com
BAKER & HOSTETLER, LLP
11601 Wilshire Boulevard, Suite 1400
Los Angeles, CA 90025
T: 301.820.8800 / F: 310.820.8859

Fernando A. Bohorquez, Jr. (*Pro Hac Vice pending)*
BAKER & HOSTETLER, LLP
45 Rockefeller Plaza
New York, N.Y. 10111
T: 212.589.4200 / F: 212.589.4201

Jose Perez (*Pro Hac Vice pending)*
LatinoJustice PRLDEF
99 Hudson Street, 14th Floor
New York, NY 10013
T: 212.219.3360 / F: 212.431.4276

Attorneys for *Amicus Curiae*
LATINOJUSTICE PRLDEF, et al.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA and JANET NAPOLITANO, *in her official capacity as President of the University of California,*

Plaintiffs,

v.

U.S. DEPARTMENT OF HOMELAND SECURITY and ELAINE C. DUKE, in her official capacity as Acting Secretary of Homeland Security,

Defendants.

AND ADDITIONAL CASES.

Case No. 17-CV-05211-WHA
Case No. 17-CV-05235-WHA
Case No. 17-CV-05329-WHA
Case No. 17-CV-05380-WHA
Case No. 17-CV-05813-WHA

Hon. William Alsup

BRIEF OF *AMICUS CURIAE* LATINOJUSTICE PRLDEF, ET AL. IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

TABLE OF CONTENTS

Page

BAKER & HOSTETLER LLP
ATTORNEYS AT LAW
LOS ANGELES

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION AND SUMMARY OF ARGUMENT[1]

This brief presents the legal and policy privacy concerns of *Amici* LatinoJustice PRLDEF, Alianza Americas, the Arab American Institute, the Asian American Legal Defense and Education Fund, Asian Americans Advancing Justice - AAJC, AAJC - Asian Law Caucus, AAJC – Los Angeles, ASPIRA, the Council on American-Islamic Relations, CUNY DREAMers, Dream Action Coalition, the Hispanic Association of Colleges and Universities, the Hispanic National Bar Association, the Hispanic Federation, Inc., Long Island Immigrants Students Advocates, The New York State Youth Leader Council, Presente.org, RU Dreamers, and Unidos US (collectively, "*Amicus Curiae"*) regarding the September 5, 2017 memorandum, issued by the Department of Homeland Security of the United States ("DHS"), rescinding the Deferred Action for Childhood Arrivals ("DACA") program established by DHS in 2012 ("DACA Rescission Memorandum").

Amicus Curiae submit this brief in support of the preliminary injunction motion brought by all plaintiffs in the consolidated DACA actions in this district ("Consolidated DACA Actions"). The Consolidated DACA Actions detail at length the constitutional and statutory violations of the DACA Rescission Memorandum. The Consolidated DACA Actions plaintiffs have moved for injunctive relief on their collective claims under the Administrative Procedure Act, 5 U.S.C. § 706 ("APA") that DHS's decision to rescind DACA was arbitrary and capricious. Among other things, the Consolidated DACA Actions allege that without any justification or reasoned rationale, the DACA Rescission Memorandum and its implementation materially deviate from DHS's prior promises concerning the government's use of personal information ("PI") provided by DACA recipients ("Dreamers") to DHS in their DACA applications. The Consolidated DACA Actions' preliminary injunction motion and supporting declarations establish that (1) Dreamers relied on DHS's repeated assurances that the PI collected for the purpose of providing DACA relief would be protected from disclosure to U.S. Immigration and

[1] Per the Court's October 25, 2017 Order, the *Amicus Curiae*'s Statement of Interest is included in the *Amicus Curiae's* Motion for Leave. Generally, *Amici* are a collection of civil rights defense funds, immigrant rights groups, policy, advocacy and community service organizations, and student groups, who represent the interests of DACA recipients and in many cases are comprised of leaders and members who are themselves DACA recipients.

Customs Enforcement ("ICE") and not be used for immigration enforcement purposes, absent exceptional circumstances; and (2) the DACA Rescission Memorandum removes those protections and now allows Dreamers' PI to be shared with ICE and used against them for the purposes of removal—the precise opposite of DHS's representations to the Dreamers at the time DHS solicited their PI. As demonstrated below, DHS's retroactive material change in its data usage policy concerning the use of Dreamers' previously collected PI violates long-standing privacy principles—including the agency's own policies—and therefore violates the APA.

Dreamers—including many of the leaders and members of several *Amici*—provided an exhaustive list of PI in their DACA applications including, but not limited to, date and place of birth, alien registration number, U.S. home address, school name and location, a detailed history of any minor criminal offenses, including arrests or convictions, and biometric information such as fingerprints and photos. DHS made repeated assurances on its online DACA "Frequently Asked Questions" ("DACA FAQs"), that PI would "be protected from disclosure to ICE … for the purpose of immigration enforcement" with limited exceptions where "the requestor meets the criteria for the issuance of a Notice To Appear ["NTA"] or a referral to ICE under the [NTA] criteria."[2] The DACA FAQs also represented that, except in limited circumstances, "[i]f you have submitted a request for consideration of DACA and USCIS decides not to defer your case . . . your case **will not** be referred to ICE for purposes of removal proceedings."[3] Relying on DHS's assurances concerning these data use limitations, Dreamers provided their PI to DHS in their DACA applications. Additionally, Dreamers provided sensitive arrest and misdemeanor records only under assurances that DHS did not view such information as a bar to DACA qualification or as a threat for removal, as they were of the lowest enforcement priority. Importantly, after DACA's implementation, and consistent with U.S. government privacy principles, DHS Secretary Jeh Johnson wrote to Congress that "these representations made by the U.S. government, upon which DACA applicants most assuredly relied, must continue to be honored."[4]

[2] *See* DHS DACA FAQs, U.S. Citizenship and Immigration Services Q19 (last updated Oct. 6, 2017), *https://www.uscis.gov/archive/frequently-asked-questions*.
[3] *Id*. at Q26 (emphasis added).
[4] *See* Letter to Judy Chu, U.S. House Representative, from Jeh Johnson, Dept. of Homeland Sec. Secretary (Dec. 30, 2016) *available at*

On September 5, 2017, DHS rescinded the DACA program without obtaining consent from, or providing notice and opportunity for comment to Dreamers or the public. *See* Admin. R. at 252-56. The DACA Rescission Memorandum does not reflect any consideration of the impact DHS's action may have on the Dreamers' privacy interests, much less reference any privacy impact assessment or DHS's compliance with any internal privacy policies or practices.[5] DHS simultaneously posted revised "Frequently Asked Questions," (the "Rescission FAQs") that materially changed the prior policy as to the treatment of PI previously provided by Dreamers, and applied this new policy retroactively.[6] The Rescission FAQs state: "Generally, information provided in DACA requests will not be proactively provided to other law enforcement entities (including ICE and CBP) for the purpose of immigration enforcement proceedings unless the requestor poses a risk to national security or public safety, or meets the criteria for the issuance of a Notice To Appear ["NTA"] or a referral to ICE under the [NTA] criteria."[7] Critically, the Rescission FAQ's remove DHS's prior express representations that Dreamers' PI would be explicitly protected from disclosure to ICE for purposes of immigration enforcement and not be referred to ICE for purposes of removal.

To make matters worse, DHS radically broadened the categories of people to be prioritized for removal in its February 20, 2017 Enforcement Priorities Memorandum. *See* Admin. R. at 226-34. Previously, DHS prioritized removing individuals who had been convicted of felonies or serious (or multiple less serious) misdemeanors. The Enforcement Priorities Memorandum expanded the categories to include those who "(1) have been convicted of **any** criminal offense; (2) have been **charged** with any criminal offense that has not been resolved; [and] (3) have **committed acts** which constitute a chargeable criminal offense." *Id.* at 230. In other words, individuals not convicted of, but only charged with, any criminal offense are now

---

https://chu.house.gov/sites/chu.house.gov/files/documents/DHS.Signed%20Response%20to%20Chu%2012.30.16.pdf.

[5] *Id.*

[6] *See* Frequently Asked Questions: Rescission Of Deferred Action For Childhood Arrivals (DACA), Dept. of Homeland Sec. (Sept. 5, 2017), https://www.dhs.gov/news/2017/09/05/frequently-asked-questions-rescission-deferred-action-childhood-arrivals-daca.

[7] *Id.* at Q8.

prioritized for immigration enforcement. This includes various lower-level offenses that Dreamers freely disclosed as part of their DACA applications.[8]

Given the DACA Rescission Memorandum, the material change in data usage protection afforded DACA PI in the Rescission FAQs, and DHS's broadened enforcement priorities, Dreamers have a well-founded fear that their PI will be disclosed to ICE and used against them for removal. As demonstrated below, the disclosure of Dreamers' PI to ICE for deportation purposes contravenes the Fair Information Practice Principles (FIPPs) that the DHS has historically adopted and endorsed as part of its privacy policies and practices. These principles—reflected in DHS privacy policy memoranda, the Privacy Act of 1974, and the privacy policy reports and enforcement actions of the Federal Trade Commission—hold that the government is limited to using PI it collects from individuals for its original purpose, and cannot subsequently use such PI for purposes incompatible with the goals of the initial collection. As applied to DACA, Dreamers provided their PI to DHS for the purposes of obtaining temporary lawful status and work authorization for two years, and DHS promised that such information would not be used to remove them. Yet, that is precisely what DHS threatens to do now. This threat violates the fundamental privacy principle that the government cannot collect information for one purpose and later use it for a materially different one, much less for a purpose it expressly promised that data would not be used for. Accordingly, *Amicus Curiae* respectfully urge the Court to grant plaintiffs' motion for preliminary injunction on the grounds that the DACA Rescission Memorandum violates the APA as arbitrary and capricious, and enjoin DHS from using PI provided under DACA for immigration enforcement purposes.

///

///

///

[8] Although the Enforcement Priorities Memorandum exempted the DACA program, the DACA Rescission Memorandum is silent on whether the exemption applies after DACA ends.

II. ARGUMENT

A. PRIVACY PRINCIPLES PROVIDE THAT THE GOVERNMENT IS LIMITED TO USING PERSONAL INFORMATION FOR THE PURPOSE REPRESENTED AT THE TIME OF COLLECTION OF SUCH PERSONAL INFORMATION.

1. The Fair Information Practice Principles and DHS Endorsement of the Purpose Specification and Use Limitation Principles

DHS has explicitly adopted the long-standing and widely accepted privacy principles known as the Fair Information Practice Principles, or FIPPs, as the framework for its privacy compliance policies and procedures.[9] The FIPPs form the backbone of privacy and data protection laws in the United States and originate from the Privacy Act of 1974, 5 U.S.C. § 552a (2012) (the "Privacy Act").[10] The eight principles address the manner in which PI is collected and used, and provide safeguards to assure those practices are fair, non-deceptive, and adequately protect PI. The most relevant FIPPs here, as explained by DHS, are:

> **Transparency** – Transparency should be provided as to how PI is handled via various mechanisms, including general notices, reports, investigations, public meetings, Privacy Impact Assessments ("PIA"), System of Records Notices ("SORN"), and the Freedom of Information Act ("FOIA").[11]
>
> **Purpose Specification –** The purposes for which PI is collected must be clearly specified at the time of collection and the subsequent use of the PI must be compatible with the fulfillment of those purposes.[12]
>
> **Use Limitation –** PI should only be used for the purposes specified at the time of collection, and not be disclosed, made available, or otherwise used for any other purposes, in accordance with the Purpose Specification Principle.[13]

In January 2009, DHS issued an amended version of its privacy policy guidance memorandum making it clear that any PI "collected, used, maintained, and/or disseminated by DHS" would be "subject to the Privacy Act regardless of whether the information pertain[ed] to a

---

[9] *See* Memorandum from Hugo Teufel III, Chief Privacy Officer, U.S. DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM NO. 2008-01 (December 29, 2008) ("2008 Privacy Policy Memorandum"), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

[10] *See* Privacy Act of 1974, 5 U.S.C. § 552a, as amended; Homeland Security Act of 2002, as amended, 6 U.S.C. § 142;*see also* Memorandum from Jonathan R. Cantor, Acting Chief Privacy Officer, U.S. DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM NO. 2017-01 at *3 (April 25, 2017) ("2017 Privacy Policy Memorandum"), *available at* https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed _0.pdf.

[11] 2017 Privacy Policy Memorandum at *3.

[12] *Id.*

[13] *Id.* at *5-6.

U.S. citizen, legal permanent resident, visitor, or alien."[14] However, this policy materially changed on January 25, 2017, when President Donald J. Trump issued an executive order directing federal agencies "to the extent consistent with applicable law," to ensure that "their privacy policies *exclude[d]* persons who are not United States citizens or Lawful Permanent Residents ("LPRs") from the protections of the Privacy Act regarding personally identifiable information."[15] To that end, then-DHS Secretary John Kelly issued the Enforcement Priorities Memorandum on February 20, 2017, stating that DHS would no longer extend Privacy Act rights and protections to individuals who are neither U.S. citizens nor lawful permanent residents while explicitly excluded DACA recipients. Admin. R. at 229-234. The Enforcement Priorities Memorandum further directed the DHS Privacy Office to rescind the 2009 Privacy Policy Memorandum and to develop new guidance on the agency's collection, use, retention, and dissemination of PI. *Id.*

On April 25, 2017, DHS issued a memorandum updating its PI privacy policies and procedures (the "2017 Privacy Policy Memorandum").[16] While the rights and protections of the Privacy Act were no longer extended to non-citizens other than Dreamers, the 2017 Privacy Policy Memorandum reiterated DHS's commitment to the FIPPs, stating that DHS would still "treat all persons, regardless of immigration status" in a manner "consistent with the [FIPPs] and applicable law."[17] As explained in the 2017 Privacy Policy Memorandum, with respect to the Transparency principle, the agency "must provide transparency for how it handles PI through various mechanisms, including Privacy Impact Assessments (PIA), Privacy Act Statements, [and] general notices …"[18] DHS has held itself to the traditional privacy practice of providing "notice

[14] *See* Memorandum from Hugo Teufel III, Chief Privacy Officer, U.S. DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM NO. 2007-1 at *2 (January 7, 2009) (as amended from January 19, 2007) ("2009 Privacy Policy Memorandum"), *available at* https://www.dhs.gov/xlibrary/assets/privacy/ privacy_policyguide_2007-1.pdf.
[15] *See* Executive Order: Enhancing Public Safety in the Interior of the United States, The White House Press Secretary (Jan.25, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.
[16] S*ee* 2017 Privacy Policy Guidance Memorandum at *1.
[17] *Id.*
[18] *Id.* at *3.

to [an] individual regarding its collection, use, dissemination, and maintenance of personally identifiable information."[19]

Consistent with the principle of "Purpose Specification," DHS adopted the position that it "must also clearly state the purpose for which information is intended to be used in applicable … notices [and] [p]lanned uses *must be compatible with the purpose for which the Department originally collected the information; the PIA must identify and explain this compatibility."*[20] Similarly, when endorsing the "Use Limitation" principle, DHS explained "any sharing of such information outside the agency must be *compatible with the purposes for which the information was originally collected*."[21] Indeed, "ensur[ing] that such uses are compatible with the purpose for why the Department collected the records," complies with the "routine use" exception under the Privacy Act.[22] Notably, it is DHS policy that "seeking consent is always a preferable privacy practice, and consent should be sought when practical."[23] The Q & A to the 2017 Privacy Policy Memorandum states that DHS's privacy policies "permits the sharing of information about immigrants and non-immigrants with federal, state, and local law enforcement," but require that "such sharing conform to an analysis based upon the [FIPPs] that demonstrates a consistent relationship between the purpose for collection of the information and intended use."[24]

2. The Privacy Act's Routine Use Exception Requires That the Government's Use of Information Be Compatible with the Original Purpose of its Collection

The Privacy Act of 1974 is generally characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and

[19] *See* 2008 Privacy Policy Memorandum at *3. DHS conducts PIAs whenever a program update implicates privacy concerns to identify and mitigate privacy risks and notify the public what PI DHS is collecting, why the PI is being collected, and how the PI will be used, shared, and stored. *See* Memorandum from Hugo Teufel III, Chief Privacy Officer, U.S. DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM NO. 2008-02 (Dec. 30, 2008) *available at* https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-02_0.pdf.
[20] S*ee* 2017 Privacy Policy Memorandum at *4 (emphasis added).
[21] *Id.* at *5.
[22] *Id.* at *6 (citing 5 U.S.C. § 552a (a)(7), (e)(4)(D); *Britt v Naval Investigative Service,* 886 F.2d 544 (3rd Cir. 1989)).
[23] *See* 2017 Privacy Policy Memorandum at *6.
[24] *See* Privacy Policy 2017-01 Questions & Answers, Dept. of Homeland Sec. Q6 (April 27, 2017), *available at* https://www.dhs.gov/sites/default/files/publications/Privacy%20Policy%20Questions%20%20Answers%2C%2020170427%2C%20Final.pdf.

dissemination of PI by federal executive branch agencies.[25] The Privacy Act applies to any "system of records," which is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[26] The purpose of the Privacy Act is "to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them."[27] Although the Dreamers as non-citizens do not have a cause of action under the Privacy Act, the statute regulates the government's use of PI and therefore provides relevant guideposts in determining whether DHS's action here is arbitrary and capricious under the APA.

The Privacy Act explicitly prohibits the disclosure of PI collected by a federal agency without written consent. The Privacy Act provides that "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[28] The Privacy Act lists twelve exceptions that allow the disclosure of personal records without an individual's written consent. Of most relevance here is the "routine use" exemption, which provides that disclosure may be permitted when "the use of such record for *a purpose which is compatible with the purpose for which it was collected*."[29] (emphasis added). It was Congress's intent that the routine use exception "should serve as a caution to agencies to think out in advance what uses it (sic) will make of information."[30]

The courts have rigorously applied the compatibility requirement of the Privacy Act's routine use exception. For instance, in *Britt,* the government asserted "disclosure need only be compatible with [the routine use] purpose" published in the Federal Register, but the Third Circuit made clear that the statutory requirement of compatibility is a strict one. 886 F.2d 544,

[25] *See* Overview of the Privacy Act of 1974 at *4, U.S. DEP'T OF JUSTICE (2015 Edition), *available at* https://www.justice.gov/opcl/file/793026/download.
[26] *See* 5 U.S.C. § 552a (a)(5).
[27] *See* Litigation Under the Privacy Act at § 2, 114 AM. JUR. TRIALS 89 (2009).
[28] S*ee* 5 U.S.C. § 552a (b).
[29] *See* 5 U.S.C. § 552a (a)(7).
[30] *See Britt,* 886 F.2d 544, 548 (3rd Cir. 1989) (citations omitted).

548-9. Instead, compatibility "requires [] a dual inquiry into the purpose for the collection of the record in the specific case and the purpose of the disclosure." *Id.* (finding the collection of information for purposes of criminal investigation was not compatible with disclosure to government agency employer, for use by employer in evaluating employee's integrity).

Case law uniformly holds that "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure." *Id.* at 549-50. The Ninth Circuit's holding in *Covert v. Harrington* is particularly instructive here, finding that the Department of Energy ("DOE")'s disclosure of employee personnel security questions ("PSQs") to the Department of Justice ("DOJ") was unauthorized under the Privacy Act.[31] 876 F.2d 751, 755 (9th Cir. 1989). In *Covert*, the DOE had originally collected personal information from employees in the PSQ's to determine their eligibility for security clearances. *Id* at 752-53. The district court found that DOE's disclosure to DOJ of the employee's PSQs for law enforcement purposes was not a routine use, as it was not compatible with the use for which the information was originally collected. *Id.* at 753. The Ninth Circuit affirmed, finding the failure of the government to inform employees that their personal information would be used for purposes other than stated at the time of collection, was a violation of the Privacy Act. *Id.*

3. Under Long-Standing Federal Trade Commission Policy, Entities Must Provide Consumers with Notice of Data Use Practices and Obtain Consent When Such Use is Materially Different from When Initially Collected

The core privacy tenets of Purpose Specification and Use Limitation applied in the Privacy Act have been historically extended to other regulatory contexts. Perhaps the most important is the Federal Trade Commission ("FTC"), which has been the chief federal agency on consumer privacy policy, protection and enforcement since the 1970s.[32] While the FTC's

[31] *See also Swenson v. U.S. Postal Serv.*, 890 F.2d 1075, 1078 (9th Cir.1989) (holding that collection of data for purposes of adjudicating EEOC charges was not compatible with disclosure to Congress investigating charges brought by an employee who had filed complaint that the U.S. Postal Service had undercounted its rural routes).

[32] *See* Protecting Consumer Privacy, Fed. Trade Comm'n (last visited Oct. 27, 2017), *available at* https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy.

jurisdiction is limited to acts affecting commerce, the agency's interpretation of FIPPs is persuasive authority for the application of FIPPs generally, as well as applied to the government. The FTC's focus on online privacy began in 1998 in its first report to Congress on the issue, in which the FTC endorsed the widely-accepted FIPPs of Notice, Choice, Access, and Security, as "essential to ensuring that the collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests."[33] The 1998 FTC Report stated that "[t]hese core principles require that consumers be given *notice* of an entity's information practices; [and] that consumers be given *choice* with respect to the use and dissemination of information collected from or about them…."[34]

In its seminal 2000 Privacy Online Report to Congress, the FTC advised that organizations should provide consumers with "clear and conspicuous notice" of their privacy practices, including "what information they collect, how they collect it . . . how they use it, how they provide Choice, Access, and Security to consumers, [and] whether they disclose the information collected to other entities . .."[35] The FTC has been especially concerned with privacy policies that "reserve[] the right to make changes to its information practices in the future" and require consumers to "check the policy often for such changes," because "[t]he chance that new, inconsistent policies may be applied to previously collected information is troubling and may undermine consumer confidence in the rest of the privacy policy."[36] The FTC has made clear that consumers should be informed of any "material changes" to an organization's practices as to information collection, retention, and disclosure, and in some instances, may even require consumers' "affirmative" consent to changes.[37]

[33] *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS, at *ii (June 1998) ("1998 FTC Report"), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.
[34] *Id.*
[35] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS, at * 36 (May 2000) ("2000 Online Privacy Report to Congress"), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.
[36] *Id.* at 26.
[37] *Id.*

In its 2012 Privacy Report, the FTC highlighted the privacy-related harms that might arise from unanticipated, unconsented uses of data as "more expansive than economic or physical harms," and may include "the unexpected revelation of previously private information, including both sensitive information (*e.g.*, health information, precise geolocation information) and less sensitive information (*e.g.*, purchase history, employment history) to unauthorized third parties."[38] To address these concerns, the FTC stated, in no uncertain terms, that "[c]ompanies should obtain affirmative, express consent before (1) using consumer data in a *materially different manner* than claimed when the data was collected; or (2) collecting sensitive data for certain purposes."[39] These concerns are best illustrated in the FTC's enforcement actions and settlements against Google and Facebook for retroactive material change in use.[40] The settlement agreements require that the companies give their users clear and prominent notice and "obtain affirmative express consent prior to making certain *material retroactive changes to their privacy practices*."[41] The FTC has explained that a "material change" means "at a minimum, sharing consumer information with third parties after committing at the time of collection not to share the data."[42] In the bankruptcy context, the FTC has applied this principle to find that companies' liquidations cannot transfer personal information, if the company had previously represented to consumers that such information would not be transferred at the time of collection.[43]

BAKER & HOSTETLER LLP
ATTORNEYS AT LAW
LOS ANGELES

[38] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at *8 (March 2012) ("2012 Privacy Report"), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[39] *Id.* at viii (emphasis added).

[40] The FTC alleged that Google improperly used the information provided by consumers when they signed up for Gmail to populate a new social network called "Google Buzz" without notice or consent. *Id*. at 8, n. 37. The FTC's complaint against Facebook alleged that the social network's sharing of users' personal information beyond consumer's initial privacy settings unfairly exposed potentially sensitive information to third parties. *Id.* at 8.

[41] *See* 2012 Privacy Report at 58 (emphasis added).

[42] *Id.*

[43] *See e.g.*, Letter from Fed. Trade Comm'n to Cullen and Dykman LLP (July 1, 2010), *available at* https://www.ftc.gov/system/files/documents/closing_letters/ letter-xy-magazine-xy.com-regarding-use-sale-or-transfer-personal-information-obtained-during-bankruptcy-proceeding/100712xy.pdf.

B. APPLYING PRIVACY PRINCIPLES, DHS'S MATERIAL CHANGE IN POLICY TO DISCLOSE DACA PERSONAL INFORMATION TO ICE FOR REMOVAL PURPOSES IS ARBITRARY AND CAPRICIOUS.

As adopted by DHS itself, the Purpose Specification and Use Limitation FIPPs stand for the common sense and equitable proposition that DHS is limited to using PI solely for the purposes specified when first collected, and any PI disclosure to another agency such as ICE, must be for a use compatible with the originally stated purpose. This basic principle is echoed in the Privacy Act regulating the government's collection and use of PI, which requires that use of information must be compatible with the purpose for which it was originally collected. In the consumer protection context, this privacy tenet has been historically applied by the FTC to find that companies should provide notice of their information use practices and obtain affirmative consent when such use is materially different from when the data was first provided by the consumer.

The DACA Rescission Memorandum is a strikingly arbitrary departure from these privacy principles, including the agency's own practices. As part of the DACA application process, Dreamers provided DHS sensitive PI, including country of origin, date of entry, current U.S. home address, school location, misdemeanor and arrest information, and biometric identifiers, for the limited purposes of obtaining temporary lawful status and work authorization. The DACA FAQs constituted notice of use limitations at the time of collection and explicitly provided that Dreamers' PI would not be used for deportation absent extremely limited stated exceptions and that the PI provided would be used solely for the purpose of obtaining DACA relief. What is more, the DACA FAQs expressly stated that the PI provided for DACA purposes would not be shared with ICE for the purposes of removal. In other words, the stated purpose for DHS's collection of Dreamers' PI at the time of collection was to provide applicants assurances they would not to be deported.

Yet, the DACA Rescission Memorandum and the Rescission FAQs on their face allow for that previously collected information to now be used for the precise opposite use of its original collection—the arrest and removal of Dreamers. When DHS issued the DACA Rescission Memorandum, DHS did *not* affirm that PI provided by Dreamers in their DACA applications

would not be used for any other purpose than for which it was originally collected. To the contrary, DHS posted online the Rescission FAQs, which not only failed to provide any assurances to Dreamers that their PI would not be used for immigration enforcement, but can be read to permit such use, especially against Dreamers with minor criminal offenses or even a single misdemeanor arrest.

DHS's use of PI for the purpose of removal is fundamentally *not* compatible with the purpose for which the information was originally collected – namely immigration relief – and therefore clearly violates the agency's own Purpose Specification and Use Limitation FIPPs adopted in its 2017 Privacy Memorandum and the APA as arbitrary and capricious. *See e.g., Venetian Casino Resort, L.L.C. v. E.E.O.C.*, 530 F.3d 925, 934–35 (D.C. Cir. 2008) (finding the Equal Employment Opportunity Commission's (EEOC) policy permitting agency employees to disclose employer's confidential information to potential ADEA plaintiffs without first notifying employer/submitter, was arbitrary and capricious under the APA because the policy conflicted with EEOC regulations). It also flies in the face of well-established court precedent interpreting the Privacy Act's routine use exception as requiring that agency use must be compatible with the purpose for which the information was collected. *See*, Part I.B, *supra.*

Further, DHS's decision to rescind DACA without any notice, consent, or even the opportunity to comment violates the agency's adopted Transparency FIPP memorialized as recently as the 2017 Privacy Policy Memorandum. Neither the DACA Rescission Memorandum nor anything in the administrative record before the court on this motion, remotely suggests that DHS even considered the impact on Dreamers' privacy interests, much less conduct a PIA on how the Dreamers' privacy rights may be affected. Moreover, DHS materially changed its data use policies to allow for the use of Dreamers' PI for enforcement purposes without notice and without consent from any Dreamers. The FTC, as the government's privacy watchdog, has traditionally held that entities must notify consumers and obtain affirmative consent when making material retroactive changes to their privacy practices. DHS fell far short of meeting that standard here. Indeed, it would not be an overstatement to say that if DHS were a commercial entity, the FTC would find DHS's retroactive material change in use of Dreamers' previously collected PI to

be a deceptive trade practice, which must be tantamount to an arbitrary and capricious agency action.

C. CONCLUSION

Accordingly, *Amicus Curiae* respectfully urge the Court to grant plaintiffs' motion for preliminary injunction on the grounds that the DACA Rescission Memorandum violates the APA as arbitrary and capricious, and enjoin DHS from using PI provided under DACA for immigration enforcement purposes.

Dated: November 1, 2017

BAKER & HOSTETLER, LLP

By: */s/ Blythe G. Kochsiek*
Alan L. Friel
Blythe G. Kochsiek

Of Counsel:
Fernando A. Bohorquez, Jr. (*Pro Hac Vice pending)*
BAKER & HOSTETLER, LLP

Jose Perez (*Pro Hac Vice pending)*
LatinoJustice PRLDEF

Attorneys for *Amicus Curiae*
LATINOJUSTICE PRLDEF et al.

CERTIFICATE OF SERVICE

The undersigned, an attorney, hereby certifies that he served a copy of the foregoing on all counsel of record via the Court's CM/ECF system.

Dated: November 1, 2017

/s/ Blythe G. Kochsiek
Blythe G. Kochsiek