DEPARTMENT OF JUSTICE
Federal Bureau of Investigation

AAG/A Order No. 028-2007
Privacy Act of 1974; Notice to Amend System of Records

Terrorist Screening Records System

COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION

In 2005, the Federal Bureau of Investigation ("FBI") established a system of records known as the Terrorist Screening Records System ("TSRS") to encompass the government's consolidated terrorist watch list information, operational support records, and records related to complaints or inquiries.[1] The FBI also exempted the TSRS from several provisions of the Privacy Act, which eliminated many rights and protections that United States citizens and permanent residents would otherwise have in information maintained about them in the TSRS.[2] On August 22, 2007, the FBI published a notice to amend certain aspects of this system of records.[3] Pursuant to the August 22 notice, the Electronic Frontier Foundation ("EFF") submits these comments to address the substantial due process and privacy issues raised by government watch lists and other information contained in the TSRS, and to urge the agency to revisit its claimed Privacy Act exemptions to address these crucial issues.

The TSRS contains classified and unclassified information about several categories of people, including known or suspected terrorists, individuals who are

---

[1] Final Rule, 70 Fed. Reg. 72199 (Dec. 2, 2005).

[2] *Id.*

[3] Notice to Amend System of Records, 72 Fed. Reg. 47073 (Aug. 22, 2007).

screened by the Terrorist Screening Center as possible watch list matches, individuals who are misidentified as watch list matches, individuals who submit redress inquiries, and information about encounters with all of these individuals.[4] The system is used to make determinations that fundamentally affect individuals' lives, such as whether they may fly on airplanes, enter the United States, obtain United States citizenship, or be arrested.[5] Despite its potential impact on the lives of millions of citizens, the system is known to contain to contain inaccurate, incomplete, untimely, irrelevant and unnecessary information. Citizens may not be able to access or correct this information, particularly because they have no judicially enforceable right of redress for negative determinations made on the basis of certain information in this system. In short, the TSRS is exactly the sort of records system Congress intended to prohibit when it enacted the Privacy Act of 1974.[6]

Introduction

The Terrorist Screening Center ("TSC") is a multi-agency effort spearheaded by the FBI that has been tasked with consolidating several watch lists into a single database.[7] The purpose of the TSC is to enhance the government's ability to "protect the people, property, and territory of the United States against acts of terrorism."[8] The Terrorist

[4] 72 Fed. Reg. 47073, 47076.

[5] *Id*.

[6] 5 U.S.C. § 552a.

[7] Congressional Research Service, RL32366, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6* 2 (Apr. 21, 2004).

[8] The White House, *Homeland Security Presidential Directive/HSPD-6, Integration and Use of Screening Information* (Sept. 16, 2003), http://www.whitehouse.gov/news/

Screening Database ("TSDB") — a large component of the TSRS — contains information from twelve government watch lists maintained by the Department of State, Department of Homeland Security ("DHS"), Department of Justice, FBI, Marshals Service, Department of Defense, and the Air Force.[9] According to the Department of Justice Inspector General ("DOJ IG"), "the number of watchlist records contained in the TSDB has more than quadrupled since [the database's] inception in 2004."[10] The consolidated watch list is a central factor of other government programs such as Secure Flight, the Transportation Security Administration's proposed air passenger prescreening program that will "screen" tens of millions of travelers.[11]

The U.S. Supreme Court has long recognized that citizens enjoy a constitutional right to travel. Thus, in *Saenz v. Roe*, the Court noted that the "constitutional right to travel from one State to another is firmly embedded in our jurisprudence."[12] For that reason, any governmental initiative that conditions the ability to travel upon the surrender

---

releases/2003/09/20030916-5.html.

[9] Department of Justice, Inspector General, Audit Division, Audit Report No. 05-27, *Review of the Terrorist Screening Center* iii (June 2005) (hereinafter "2005 DOJ IG Report"). Two watch lists that have become part of the TSDB are the Department of Homeland Security's "no-fly" and "selectee" lists, which have been long known to pose misidentification problems that passengers find difficult, if not impossible, to resolve.

[10] Department of Justice, Inspector General, Audit Division, Audit Report No. 07-41, *Follow-up Audit of the Terrorist Screening Center* 7 (Sept. 2007) (hereinafter "2007 DOJ IG Report").

[11] Notice of Proposed Rulemaking, 72 Fed. Reg. 48397 (Aug. 23, 2007); Notice to Establish System of Records, 72 Fed. Reg. 48392 (Aug. 23, 2007); Notice of Proposed Rulemaking, 72 Fed. Reg. 48356 (Aug. 23, 2007).

[12] 526 U.S. 489, 498 (1999), quoting *United States v. Guest*, 383 U.S. 745, 757 (1966) (internal quotation marks omitted).

of privacy rights requires particular scrutiny. This concern is particularly relevant to the use of watch list information in the context of aviation security. When the DOJ IG conducted a review of the TSDB in June 2005, it concluded that the system suffered from major flaws in data accuracy and completeness, among other things.[13] The IG's recent follow-up review of the system confirmed that the watch list continues to be plagued by problems, including significant data quality and redress issues.[14]

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and, significantly, required agencies to be transparent in their information practices.[15] The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[16] Adherence to these requirements is particularly critical for a system like TSRS, the operation of which can have major implications for data subjects.

EFF commends the FBI for proposing certain changes to the TSRS intended to promote "appropriate oversight of the proper use of TSC data systems."[17] Among other positive steps, the FBI is amending the system to add audit logs as a new category of

---

[13] 2005 DOJ IG Report, *supra* note 9, at 66-67.

[14] 2007 DOJ IG Report, *supra* note 10, at ii.

[15] S. Rep. No. 93-1183, at 1 (1974).

[16] *Id*.

[17] 72 Fed. Reg. 47073, 47075.

information, which may help limit the potential misuse of the TSRS.[18] The agency is also proposing to maintain archived records and histories, in part to facilitate redress, data quality assurance, and for oversight and auditing purposes.[19] While these records should certainly be retained for less than 50 years, as the FBI proposes,[20] these efforts to build greater accountability into the system are positive changes.

Unfortunately, portions of the TSRS continue to be exempt from many critical Privacy Act rights and protections, which is particularly troubling in light of the fact that the system has had well documented data quality and redress problems since its inception. The FBI has also been unresponsive to a Freedom of Information Act ("FOIA") request for information concerning terrorist watch list misidentifications, which further indicates that the FBI is falling short of adequate accountability and transparency in its administration of the consolidated watch list.

I. The FBI Has Not Released Enough Information Public to Permit Scrutiny of Watch Lists and the Terrorist Screening Center.

As an initial matter, we note the FBI's lack of public disclosure concerning the system of records at issue in this proceeding. Since the TSDB became operational in 2004, a handful of government reports have flagged serious deficiencies in the system, the most recent of which was published just last month.[21] There is no indication,

---

[18] *Id*. at 47074.

[19] *Id*.

[20] *Id*. at 47076.

[21] *See* Government Accountability Office, GAO-05-356, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed* 31 (March 2005) (hereafter "GAO Report"); 2005 DOJ IG Report, *supra* note 9, at 66; 2007 DOJ OG Report, *supra* note 10, at ii.

however, that the Bureau has adequately addressed concerns raised by other federal offices and agencies. Furthermore The FBI itself has made public little information about the TSRS. For example, in response to a government report noting that Customs and Border Protection officers had encountered difficulties with false matches to names in the TSDB during secondary screenings at U.S. points of entry,[22] EFF submitted a Freedom of Information Act ("FOIA") request to the FBI to obtain the public release of additional information concerning the TSC's watch list matching operations.[23] More than a year later, the FBI has not responded to the request.

Because the information in the public record indicates that the TSDB continues to have serious shortcomings, and because the FBI has not provided adequate information about the current state of the TSDB, EFF urges the FBI not to expand the system or increase other entities' reliance on it in any way until the public is able to verify that the TSDB has been significantly improved. The Bureau's refusal to release responsive information about the operation of watch list frustrates the ability of the public to submit meaningful, well-informed comments in response to this notice. In order for this notice and comment period to be anything other than a perfunctory exercise, the time for comment should be extended until the Bureau is willing to release more substantial information about the consolidated watch list and its use in other government programs

---

[22] Department of Homeland Security, Office of Inspector General, OIG-06-43, *Review of CBP Actions Taken to Intercept Suspected Terrorists at U.S. Ports of Entry* 3-4 (June 2006).

[23] Letter from Marcia Hofmann, Staff Attorney, Electronic Frontier Foundation, to David M. Hardy, Chief, Record/Information Dissemination Section, Records Management Division, FBI, Aug. 30, 2006 (on file with EFF).

such as Secure Flight. The continuing lack of transparency surrounding the current functionality of the TSRS requires the FBI to 1) make additional details concerning the state of the consolidated watch list available to the public; and 2) provide further opportunity for public comment on the TSRS once more substantial details about the system are revealed.

II. The TSRS Continues to Contradict the Intent of the Privacy Act.

The Privacy Act was intended to guard citizens' privacy interests against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[24] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[25] As we detail below, the exemptions claimed by the FBI for the TSRS are thoroughly inconsistent with the purpose and intent of the Privacy Act.

A. The FBI's Privacy Act Exemptions for the TSRS Permit the Agency to Collect and Maintenance Inaccurate, Untimely, Incomplete, Irrelevant, and Unnecessary Information.

The TSC is required to "develop and maintain, to the extent permitted by law, the most thorough, accurate, and current information possible about individuals" related to

[24] Pub. L. No. 93-579 (1974).

[25] *Id.*

terrorism.[26] It is thus deplorable that the FBI exempted the TSRS in 2005 from the fundamental Privacy Act requirement that it "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[27] To make matters worse, the FBI has also exempted the system from the obligation that an agency "maintain in its records only such information about an individual as is relevant and necessary" to achieve a stated purpose required by Congress or the President.[28] Such open-ended, haphazard data collection plainly contradicts the objectives of the Privacy Act and raises serious questions concerning the potential impact of the TSC screening process on millions of law-abiding citizens.

The TSC's refusal to ensure the accuracy of the data in the TSRS is particularly troubling in light of evidence that the consolidated watch list is rife with inaccuracies. For instance, a TSC official informed the Government Accountability Office in 2005 that approximately 4,800 individuals' records had been purged from the consolidated watch list, presumably because they did not belong there.[29] Furthermore, the DOJ IG reported the same year:

> our review of the consolidated watch list identified a variety of issues that contribute to weaknesses in the completeness and accuracy of the data,

---

[26] *Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism* 1 (Sept. 16, 2003).

[27] 5 U.S.C. § 552(a)(e)(5).

[28] 5 U.S.C. § 552a(e)(1); 70 Fed. Reg. 43661.

[29] GAO Report, supra note 21, at 31.

> including variances in the record counts between [two versions of the Terrorist Screening Database], duplicate records, missing or inappropriate handling instructions or categories, missing records, and inconsistencies in identifying information between TSDB and source records."[30]

More recently, the TSC determined last year that the TSDB contained more than 2,100 records that "did not belong in the TSDB and needed to be removed from the consolidated watchlist."[31] Regardless, "[d]espite being responsible for removing outdated or obsolete data from the TSDB . . . the TSC did not have a process for regularly reviewing the contents of the TSDB to ensure that the database does not include records that do not belong on the watchlist."[32] Though the IG's report indicated that the TSC has taken steps over the years to improve data accuracy,[33] it is unclear that the TSDB's problems have been fully resolved. These issues are likely to exacerbated by the FBI's recently announced data retention policy for the TSDB, under which the Bureau intends to preserve information for unnecessarily long periods of time — 99 years for active records, and 50 years for inactive records.[34]

As the Office of Management and Budget noted in its guidelines for Privacy Act implementation, "[t]he objective of [requiring agencies to maintain reasonable data quality] is to minimize, if not eliminate, the risk that an agency will make an adverse determination about an individual on the basis of inaccurate, incomplete, irrelevant, or

---

[30] 2005 DOJ IG Report, *supra* note 9, at 66.

[31] 2007 DOJ IG Report, *supra* note 10, at 17.

[32] *Id*. at 18.

[33] 2005 DOJ IG Report, *supra* note 9, at 115-128; 2007 DOJ IG Report, *supra* note 10, at xi.

[34] 72 Fed. Reg. 47073, 47076.

out-of-date records that it maintains."[35] Maintaining the most accurate possible data is unquestionably a critical goal for the TSRS, since a false negative match to the consolidated watch list could fail to detect a known a terrorist, while a false positive match could erroneously label an innocent citizen a terrorist. It would therefore benefit the Bureau to observe the Privacy Act's accuracy requirements as carefully as possible, rather than exempt itself from the responsibility to maintain accurate records.

Furthermore, in adopting the Privacy Act, Congress was clear in its belief that the government should not collect and store data without a specific, limited purpose. The "relevant and necessary" provision

> reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statutes . . . . This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary[.][36]

As OMB declared in its Privacy Act guidelines, "[t]he authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful."[37] The Privacy Act's "relevant and necessary" provision thus seeks to protect individuals from overzealous, arbitrary and unnecessary data collection. It embodies the common sense principle that government data collection is likely to spiral

---

[35] Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28964 (July 9, 1975) (hereafter "OMB Guidelines").

[36] S. Rep. No. 93-3418, at 47 (1974).

[37] OMB Guidelines, *supra* note 34, at 28960.

out of control unless it is limited to only that information which is likely to advance the government's stated (and legally authorized) objective. Like the FBI's other deviations from customary Privacy Act requirements, the "relevant and necessary" exemption serves only to increase the likelihood that the TSRS will be an error-filled, invasive repository of all sorts of information bearing no relationship to terrorist screening. The Bureau should be particularly sensitive to this issue because the maintenance of information that is neither relevant nor necessary to achieve the TSC's stated goals encourages "mission creep" — the tendency of government agencies to expand the use of personal information beyond the purpose for which it was initially collected. It is crucial that the FBI strictly limit the use of collected information to the TSC's core mission.

B. The TSRS Continues to Fail to Provide Meaningful Citizen Access to Personal Information and Correction of Inaccurate Data.

In 2005, the FBI exempted the TSRS from Privacy Act provisions ensuring that citizens have the right to access records containing information about them.[38] These provisions guarantee, among other things, that an individual may request access to records an agency maintains about him or her.[39] In lieu of the statutory, judicially enforceable right of access provided by the Act, however, the Bureau has determined that requests for access to non-exempt records may be mailed to the Record Information Dissemination Office.[40] No timelines are specified for the procedure, and the process is

[38] 70 Fed. Reg. 72199, 72203.

[39] 5 U.S.C. § 552a(d)(1). Individuals generally have the right to seek judicial review to enforce the statutory right of access provided by the Act under 5 U.S.C. § 552a(g), but the FBI has exempted the TSRS from this provision, as well.

[40] 72 Fed. Reg. 47073, 47078.

left entirely to the agency's discretion.[41] The FBI's weak access provisions are in direct conflict with the purposes of the Privacy Act, which sought to provide citizens with an enforceable right of access to personal information maintained by government agencies. Furthermore, individuals who are not permitted to know what information the TSRS maintains about them are severely restricted in their ability to correct inaccurate, incomplete, and untimely information — which is particularly troubling here, since the TSDB has been found to contain "information about individuals that should not be watchlisted and . . . some watchlist records are inaccurate and complete."[42]

It follows naturally that the right to correct information is just as important as the right to access it. Unfortunately, the agency also exempted the TSRS from the Privacy Act requirements that government allow citizens to challenge the accuracy of information contained in their records, which include an agency's obligation to correct identified inaccuracies promptly, and the requirement that an agency make notes of requested amendments within the records.[43] This is particularly alarming in light of the DOJ IG's recent finding that as of April 2007, the TSC had not implemented a review process to ensure that only proper and up-to-date information is contained in the TSDB,[44] and 38 percent of TSDB records reviewed through routine quality assurance procedures still contained inaccuracies or inconsistencies.[45]

---

[41] In fact, the DOJ IG recently found that the TSC's redress processes are "not always completed in a timely manner." 2007 DOJ IG Report, *supra* note 10, at iv.

[42] 2007 DOJ IG Report, *supra* note 10, at iv.

[43] 5 U.S.C. § 552a(d)(4).

[44] 2007 DOJ IG Report, *supra* note 10, at viii.

[45] *Id*. at xii.

The rights of access and correction were central to what Congress sought to achieve through the Privacy Act:

> The committee believes that [the access and correction] provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[46]

Instead of the judicially enforceable right to correction set forth in the Privacy Act,[47] the FBI has established its own discretionary procedure for individuals to contest the accuracy of their records.[48] The FBI's Federal Register notice explains that the agency has the *discretion* to correct erroneous information upon an individual's request, but the agency has no *obligation* to do so.[49] This correction process offers a token nod to the principles embodied in the Privacy Act, but does not provide a meaningful avenue to pursue correction and is subject to change at the FBI's whim.

As the DOJ IG has noted, "[i]naccurate, incomplete, and obsolete information increases the chances of innocent persons being stopped or detained during an encounter because of being misidentified as a watchlist identity."[50] Incredibly, however, the Bureau disclaims responsibility for dealing with complaints from individuals who have screening

---

[46] H.R. Rep. No. 93-1416, at 15 (1974).

[47] 5 U.S.C. § 552a(g)(1).

[48] 72 Fed. Reg. 47073, 47078.

[49] *Id*.

[50] 2007 DOJ IG Report, *supra* note 10, at iii.

difficulty believed to be due to inaccurate information maintained by the TSC:

> If individuals . . . are experiencing repeated delays or difficulties during a government screening process and believe that this might be related to terrorist watch list information, they may contact the Federal agency that is conducting the screening process in question . . . . The TSC assists the screening agency in resolving any screening complaints that may relate to terrorist watch list information, but does not receive or respond to individual complaints directly.[51]

This is a particularly outrageous position for the TSC to take when the DOJ IG recently found that the TSC received 438 redress complaints between January 2005 and February 2007 (presumably referred from other agencies), and ultimately found it appropriate to correct or delete 45% of watch list records related to the complaints.[52] Furthermore, according to the IG:

> [T]he TSC's strategic plan does not include goals for actions associated with reducing the incidence of misidentifications or the impact on misidentified persons other than that covered by the formal redress process. Considering that nearly half of all encounters referred to the TSC Call Center are negative for a watchlist match, we believe the TSC should consider misidentifications a top priority and develop strategic goals and policy specific to mitigating the adverse impact of the terrorist screening process on non-watchlist subjects, particularly for individuals who are repeatedly misidentified as watchlist identities.[53]

The consequences of the TSC's spare redress process are amplified because other agencies using the consolidated watch list (such as the Transportation Security Administration) have likewise failed to establish robust, Privacy Act-compliant redress

---

[51] 72 Fed. Reg. 47073, 47078-9.

[52] 2007 DOJ IG Report, *supra* note 10, at xix.

[53] *Id.*, *supra* note 10, at xxi.

processes for citizens adversely affected by watch list screening procedures.[54] Indeed, the Government Accountability Office flagged this problem with respect to TSA's first iteration of the Secure Flight proposal:

> TSA does not control the content of the terrorist screening database that it intends to use as the primary input in making screening decisions, and will have to reach a detailed agreement with the TSC outlining a process for correcting erroneous information in the terrorist screening database. Until TSA and TSC reach an agreement, it will remain difficult to determine whether redress under Secure Flight will be an improvement over the process currently used or if it will provide passengers with a reasonable opportunity to challenge and correct erroneous information contained in the system.[55]

It is not yet clear whether this problem has been fully addressed in the context of the revised plan for Secure Flight. It is clear, however, that the TSRS should not be used to make determinations about individuals until redress concerns are thoroughly addressed and resolved, both by the TSC and by agencies that use TSRS information for screening purposes.

C. The TSRS's Broad "Routine Uses" Exacerbate the System's Privacy Problems.

The FBI originally identified eleven categories of "routine uses" of personal information that would be collected and maintained in the TSRS, and allowed for an additional ten "blanket routine uses" that apply to this and a number of other FBI systems of records.[56] While some of these categories are clearly related to law enforcement and

---

[54] *See* Notice of Proposed Rulemaking, 72 Fed. Reg. 48397 (Aug. 23, 2007); Notice to Establish System of Records, 72 Fed. Reg. 48392 (Aug. 23, 2007); Notice of Proposed Rulemaking, 72 Fed. Reg. 48356 (Aug. 23, 2007).

[55] *Id*. at 58.

[56] 70 Fed. Reg. 43716-43717; Privacy Act of 1974; System of Records Notice, 66 Fed. Reg. 33558, 33559-33560 (June 22, 2001).

intelligence efforts to combat terrorism, others are so broad as to permit the FBI to disclose TSRS information to virtually anyone at the agency's sole discretion. In addition to law enforcement entities, the FBI anticipates that, under certain circumstances, it may disclose TSRS information to, among others:

- "owners/operators of critical infrastructure and their agents, contractors or representatives";[57]
- professional licensure authorities;[58]
- "the news media or members of the general public in furtherance of a legitimate law enforcement or public safety function as determined by the FBI;"[59]
- former DOJ employees;[60] and
- "any person or entity in either the public or private sector, domestic or foreign, where reasonably necessary to elicit information or cooperation from the recipient for use by the TSC[.]"[61]

In its August 22 notice, the FBI added yet another category to the list — "private sector entities with a substantial bearing on homeland security."[62] Taken together, the 22 categories of "routine uses" are so broadly drawn as to be almost meaningless, allowing for potential disclosure to virtually any individual, company, or government agency worldwide for a vast array of purposes.

---

[57] 70 Fed. Reg. 43715, 43716.

[58] *Id*. at 43717.

[59] 66 Fed. Reg. 33558, 33559.

[60] *Id* at 33560.

[61] 70 Fed. Reg. 43715, 43717.

[62] 72 Fed. Reg. 47073, 47073.

These "routine" disclosures are particularly alarming because, as the DOJ IG has demonstrated, the information to be disclosed may well include material that is inaccurate, irrelevant and unnecessary to any legitimate counterterrorism purpose, and the information is not subject to a meaningful redress process even if it forms the basis for negative determinations about affected individuals. The broad dissemination of TSRS information underscores the need for full transparency (and resulting public oversight), as well as judicially enforceable rights of access and correction.

Conclusion

For the foregoing reasons, EFF urges the FBI to revisit the Privacy Act exemptions that it has claimed for the TSRS system to 1) provide individuals enforceable rights of access and correction; 2) ensure the accuracy, timeliness, and completeness of information, as well as limit the collection of information to only that which is necessary and relevant; and 3) substantially limit the routine uses of collected information. Further, development of the system should be suspended until the Bureau is willing to fully disclose relevant information about the program to the public, and the agency subsequently solicits informed public comment on the privacy implications of this database.

Dated: October 1, 2007

Respectfully submitted,

Marcia Hofmann
Staff Attorney

ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

David L. Sobel
Senior Counsel

ELECTRONIC FRONTIER FOUNDATION
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009
(202) 797-9009