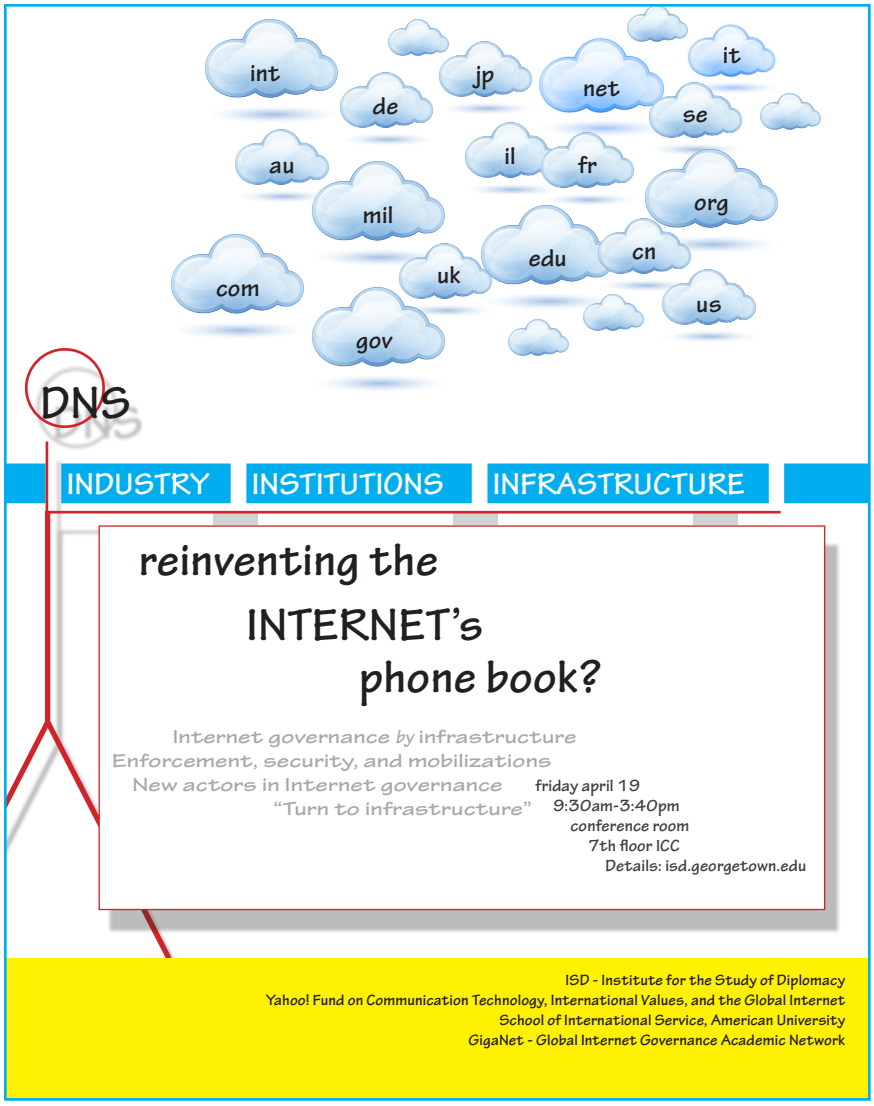

Reinventing the Internet's Phone Book? Industry, Institutions, and Infrastructure

A Conference Account

Francesca Musiani
2012–13 Yahoo! Fellow in Residence
Institute for the Study of Diplomacy
Georgetown University

With the collaboration of

Chris Haley & Allison Maranuk
2012–13 Yahoo! Junior Fellows
Master of Science in Foreign Service Program
Georgetown University

Note to the Reader: This account is intended as a follow-up resource for conference participants, for individuals who expressed interest but were unable to attend the conference, and more broadly for people interested in Internet governance, particularly DNS governance, issues. While we have paid a great deal of attention in being as accurate as possible, in no case should portions of this text be considered as direct quotes from the speakers' remarks. Thank you to all the speakers and moderators for sharing their insights, and to Chris and Allison for the diligent note-taking. I take full responsibility for whatever inaccuracy is left. FM

On April 19, 2013, the Institute for the Study of Diplomacy (ISD) at Georgetown University's School of Foreign Service hosted a conference entitled "Reinventing the Internet's Phone Book? Industry, Institutions, and Infrastructure." Since the Internet's foundation, the use of domain names, addresses, protocols, and other underlying infrastructures as instruments of power and governance has been crucial in maintaining stability throughout its evolution. In today's Internet landscape, these tools are increasingly being leveraged by political entities for purposes other than those for which they were designed. This conference set out to explore the political, social, and technical implications of this tendency, by focusing on a particularly controversial aspect of Internet infrastructure: the Domain Name System (DNS), or the Internet's "phone book." Three organizations and institutions cosponsored the event: the Yahoo! Fund on Communications Technology, International Values, and the Global Internet; American University's School of International Service; and the Global Internet Governance Academic Network (GigaNet).

Internet Governance by Infrastructure: The Case of the Domain Name System

Francesca Musiani, Yahoo! Fellow in Residence at ISD for 2012–13 and the event's host, first introduced the topic of the day's discussion. This required, initially, to briefly touch upon the definition of Internet governance (IG), which she described based on the 2005 definition by the Working Group on Internet Governance, as the development and application, by relevant actors in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet. This definition, despite its inclusiveness, has been contested by differing groups across political and ideological lines. One of the main debates concerns the authority and participation of certain actors. In particular,

the role of governments is central and ambiguous, and other aspects of Internet governance are controlled by transnational organizations. One should be careful about simplifying ideological extremes in discussing IG: the public is sometimes under the impression, fostered by the media, that IG is entirely performed by a handful of institutions—which is not the case. All of this often leads to neglect or disregard of what is, instead, a crucial aspect of Internet governance: there are a number of components of the Internet's infrastructure and technical architecture in the design of which are embedded, to some extent, arrangements of governance. These are technologies and processes beneath the layer of content and inherently designed to keep the Internet operational: Internet Protocol addresses are an example, and there are many more, but the one the conference wishes to address is the Domain Name System, or DNS.

The DNS translates between alphanumeric domain names and their associated IP addresses necessary for routing packets of information over the Internet. For this reason, it is oftentimes called the Internet's "phone book." It is a wide database management system, arranged hierarchically but distributed globally, across countless servers. The Internet's root name servers contain a master file known as the root zone file, listing the IP addresses and associated names of the official DNS servers for all top-level domains (TLDs). The management of the DNS has always been a central task of Internet governance, and the Internet Corporation for Assigned Names and Numbers (ICANN) is ultimately responsible for managing the assignment of domain names (delegated through Internet registrars), and for controlling the root server system and the root zone file.

There have been a number of controversies in this area, involving institutional and international power struggles over DNS control, and issues of legitimacy, democracy, and jurisdiction. Notably, debates have addressed the historical ties between ICANN and the United States government in face of increasing Internet globalization; this controversy continues to be a heated topic in Internet governance discussions. There are additional policy implications in the DNS: it was originally restricted to ASCII characters, precluding the possibility of domain names in many language scripts such as Arabic, Chinese, or Russian. Internationalized domain names (IDNs) have now been introduced. Furthermore, in 2011, ICANN's board voted to end most restrictions on the generic top-level domain names (gTLD) from the 22 currently available. Companies and organizations will now be able to choose essentially arbitrary top-level Internet domains, with implications for consumers' relationships to brands and ways to find information on the Internet. Further DNS issues concern the relationship between domain names and freedom of expression, security, and trademark dispute resolution for domain names.

While this covers quite a lot of ground already, this conference aimed at taking one further step. In recent years, we witness a number of (more or less successful) attempts, by political and private entities, to co-opt infrastructures of Internet governance for purposes other than the ones they were initially designed for. Not only is there governance *of* infrastructure, but governance is carried out *by* infrastructure . . . using infrastructure in "creative ways," so to speak. As DeNardis (2011) explains: "Forces of globalization and technological change have diminished the capacity of sovereign nation states and media content producers to directly control information flows. This loss of control over content and the failure of laws and markets to regain this control have redirected political and economic battles into the realm of infrastructure." Examples of how content mediation controversies have shifted into the realm of Internet governance infrastructure can be found, for example, in the intentional outages of basic telecommunications and Internet infrastructures, enacted by governments via private

actors, whether via protocols, application blocking, or termination of access services. The government-initiated Internet outages in Egypt and Libya, in the face of revolution and uprisings, have illustrated this and may have set a dangerous precedent.

However, the domain name system is perhaps, nowadays, the best illustration of this "governance by infrastructure" tendency. Domain name seizures that use the domain name system to redirect queries away from an entire web site, rather than just the infringing content, have been considered as a suitable means of intellectual property rights enforcement. DNS-based enforcement was also at the heart of controversies and Internet boycotts over the legislative efforts to pass the Protect IP Act (PIPA) and the Stop Online Privacy Act (SOPA). Governance by infrastructure enacted by private actors was also visible during the WikiLeaks saga, when Amazon and EveryDNS blocked Wikileaks' web hosting and domain name resolution services. The conference addresses these controversies, with the aim of understanding the extent to which matters of Internet governance using infrastructure entail not only issues of economic freedom—but of Internet freedoms.

The DNS Today: Enforcement, Security, and Mobilizations

The first panel, moderated by **Derrick Cogburn**, Associate Professor, School of International Service, American University, featured panelists Steve Crocker, CEO, Shinkuro, Inc. & Chair, ICANN Board, Matthew Schruers, CCIA & Adjunct Professor, Georgetown University, Scott McCormick, Consultant, McCormick ICT International, and Luke Pelican, Consultant, Ammori Group.

Dr. **Steve Crocker**, an Internet pioneer and author of the first Request for Comments of the Internet Engineering Task Force (IETF), has been involved in the development of the Internet since its startup in the late 60s and 70s. His opening remarks, he suggested, would probably be a counterpoint to the introductory talk and most of the day's discussions.

It is interesting to see how attractive the idea of Internet governance has become to such diverse groups, and the range of issues it covers. It could be useful to ask again the question: what is it that has to be governed? There are three main sets of issues.

First of all, we all have a shared interest in the system. A threat to its security is bad for the public as a whole, and maintaining operation of it is important to everyone: the system has to continue to work. Contrary to popular belief, many threats are in fact not malicious, they are accidents or otherwise caused by the overloading of the system or some of its components, and its disruption via single or multiple points of failure.

Secondly, some coordination of scarce resources is needed; however, the extent to which there are scarce resources on the Net is, in fact, debatable. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for maintaining unique identifiers in the domain name space. Originally there were 4 domains, and eventually it was decided to attach human-friendly names to those numbers. In the beginning, the majority of the connections were in the United States, with only a few international connections; since the beginning, however, there was the idea of a system as distributed as possible and over time, pressures increased to expand it. Originally, there were about 4 billion IP addresses available. In the DNS's early days, it was thought that this number would last forever—now, the IPv4 system is close to depletion. We will now see a rise of the IPv6 system, which will take some transition, and in this transition period, there may be some issues as IPv4 and IPv6 are not born interoperable.

Thirdly, some governance is needed for the suppression of undesired behavior, from impolite speech to identify theft, from espionage to extor-

tion and, of course, child pornography. This is a controversial area, of course, because "one man's freedom is another man's pain."

As the Internet began to grow, there was some conversation about who would be in charge of all this. First, Jon Postel single-handedly managed the system, simply updating the hosts.txt directory when needed. Of course, this quickly became too much, so ICANN was created and incorporated as a nonprofit in California. It has relations with the US government due to the renewal of its contract with the Commerce Department to perform the Internet Assigned Numbers Authority (IANA) functions. Today, Internet governance brings in a lot of people who want to use the Internet as a pawn in their own objectives, but are not acting in the Internet's best interest. What has made the Internet blossom is to make it as unrestricted as possible (in stark contrast to the telephone system), leaving innovation at the edges, and the same principle applies to the DNS. As there is no technical reason to either change the structure or to prohibit additional domain name systems from being created, ICANN's last "big decision" has been to lift most restrictions on gTLDs and opening up an application process.

Law scholar **Matthew Schruers** centered his remarks on the relationship between copyright and Internet architecture. As the Internet expands, the scope of government power is far more limited. Governments found it easier to regulate information intermediaries rather than the source itself. The scope of the power of the government to regulate the Internet is more about its ability to regulate the intermediaries rather than the specific sources of information. There are four regulation forces, or tools: law, norms, architecture, and markets. We are increasingly witnessing attempts to regulate architecture in order to regulate something else. SOPA and PIPA were the extension of congressional strategies to regulate intermediaries, and this included the DNS. Within these debates, and given the very different levels of technical competence on the Hill, the phone book model became really important, because it could clearly convey the idea that these laws were like removing pages from the phone book. As we will see later, SOPA and PIPA did not come into force because of widespread public outcry. These law projects would have allowed law enforcement agencies to seize domain names as if they were physical property; by removing the domain name, users would still be able to get to the website by using the IP address, but wouldn't be able to get to it by typing in the alphanumeric address—and for most people this is a big enough obstacle.

The way in which architecture regulates is not the same way in which law regulates. Norms for a particular type of conduct are very fluid, in terms of the community and how it applies; laws enforce themselves in a leaky way (especially IP law), and they need to be enforced by a judicial system. Architectural enforcement is, in this sense, "perfect": with laws, compliance is voluntary, we comply with them by choice; while with architecture-based enforcement, compliance is coerced, there is no choice. Finally, law is inherently nuanced, and there are exceptions to it; architecture is absolute, it allows a possibility or it doesn't, and there is no capacity for exceptions. The U.S. government is an example of this: recently, it used an intermediary, Go Daddy, to seize domain names in Spain; in Spain, this was lawful but in the United States it was not. Another example is the Dajaz1 website, which sometimes let out pre-releases of songs (often leaked to the website by the music promoters), so the RIAA urged the U.S. government to seize the domain via the Utah-based Fast Domain, Inc. It turned out that the legal basis, in both of these cases, was not sound, and the sites were reinstated, but in the end, free speech was suppressed a priori for two years.

Luke Pelican introduced the SOPA/PIPA controversy and the role of civil society in successfully putting a stop to the legislation. Both bills (the acronyms stand respectively for *Stop Online Piracy Act* and PROTECT IP, itself an acronym of *Preventing*

Real Online Threats to Economic Creativity and Theft of Intellectual Property Act) were aimed at combating digital piracy, and presented to the public as legislation that would help protect US. jobs and industries. Critics, on the other hand, said these bills undermined Internet freedom and threatened free speech, and could actually harm the U.S. economy, as startup companies dependent on user-created content were more likely to be sued under the legislation.

Further complicating the controversy were challenges in explaining some of the technical problems to the general public. Companies, public interest groups, and technical experts reviewed the technical provisions in the bills and raised their concerns publicly, concerns which other groups turned into meaningful action. Fight for the Future, an activist group, led a campaign against a related copyright bill in October 2011, arguing that if the bill became a law, then people like Justin Bieber could have been sent to jail instead of becoming musical successes. The "Bieber in Jail" campaign received a lot of attention from various media groups and shows like the Colbert Report. During American Censorship Day, a protest of SOPA and PIPA held on November 16, 2011, several advocacy groups framed the issue of these bills as the imposition of a U.S. censorship system rather than about the problem of piracy. The blogging platform Tumblr auto-censored its site as part of this awareness campaign and encouraged their users to contact Congress. Overall, the American Censorship Day protests resulted in 84,000 phone calls and over a million emails to Congress, one of the biggest public outcries over an Internet-related issue. It seemed to be a forgone conclusion that these bills would pass, so, on January 18, 2012, over 115,000 websites joined in a massive web "blackout" as part of a concerted effort to stop the legislation. DNS blocking provisions were included both in SOPA and in PIPA; eventually, the sponsor of the SOPA said he would remove these provisions, after talking with technical experts. The SOPA/PIPA case is likely to have encouraged more people, including lawmakers and regulators, to learn some of the technical aspects of the Internet's daily workings, and have a better understanding of how this facility we use daily works in practice. And this is a positive outcome that exceeds the stalling of the bill.

New Actors in Internet Governance: Privatization, Infrastructure, Alternatives

The afternoon panel, moderated by **Nanette Levinson**, Associate Professor, School of International Service, American University, broadened the discussion to evolutions in Internet governance and actor participation in it, from the private sector's increasingly crucial role in content regulation, and in placing restrictions on freedom of expression, to peer production collectives proposing "creative disruption" as a response to infrastructure-based enforcement. The discussion featured panelists Fiona Alexander, Associate Administrator, Office of International Affairs, National Telecommunications and Information Administration; Matthew Hindman, Associate Professor, George Washington University; Francesca Musiani, Yahoo! Fellow, ISD, and Shane Tews, Chief Policy Officer, 463 Communications.

Francesca Musiani, Yahoo! Fellow at the ISD, presented preliminary findings from her current research project. She argued that, in a discussion about new actors and changing balances in IG, it was worth including a discussion about the people who think about "second-degree" governance by infrastructure: people who, instead of addressing the DNS in its current form, look for ways to build an alternative one.

Between 2010 and 2011, the WikiLeaks case

prompts a new wave of discussions about a "new competing root-server," able to rival ICANN. An alternative domain name registry is envisaged, a decentralized, peer-to-peer (P2P) system in which volunteer users would each run a portion of the DNS on their own computer, so that any domain made temporarily inaccessible may still be accessible on the alternative registry. Instead of simply adding a number of DNS options to the ones already accepted and administrated by ICANN and its registrars, this project would try to supersede ICANN in favor of a distributed, user infrastructure-based model. There are a number of issues and open questions with this project. There are two fundamental operations that are served by the DNS: name registration and name resolution, that are usually thought of jointly, but one could foresee replacing just one of them. The function that a P2P DNS project would be tackling (alternative root? .p2p top-level domain?) needs to be stabilized. P2P architecture does not allow for simultaneous optimization of all needed features, but calls for compromises. Finally, even if the alternative takes hold, a long coexistence should be expected.

There are social and political conditions of the feasibility for radical alternatives such as P2P DNS. In the case that any of the decentralized DNS projects matures to the stage of relevant user appropriation, the crucial issue may become trust of users in other users: users will need to rely on other peers in the network to direct them, and it is one thing to trust OpenDNS, Google, etc., but completely another thing to do the same with a random computer. And finally, it is a matter of governance: the original questions that cause P2P DNS proposals to proliferate are deeply political: they are about control, freedom, and censorship. Technical solutions to controversial issues that have a political component to them should, at some point, be accompanied by evolutions of institutions, lest the governance of the Internet be reduced to a war of surveillance and counter-surveillance technologies, of infrastructure cooptation and counter-cooptation.

The "Turn to Infrastructure" and the Future of IG

In the conference's final keynote, **Laura DeNardis**, Associate Professor in the School of Communication at American University, tied together the themes discussed during the day, placing particular emphasis on recently raised concerns about the future of Internet governance, and on the need to preserve interoperability. Most of these issues are discussed in her book "The Global War for Internet Governance," forthcoming with Yale University Press. The book describes the different layers of how internet governance works; outlines the current state of global debates, and the balance of global political and economic powers related to Internet governance, civil liberties and national security, innovation policies and the preservation of the decentralized nature of the Internet.

Internet governance functions, even though technologically complex and often outside of public view, are becoming political proxies for global political struggles and conflicting values. In this context, the DNS is one important (and relatively well-working) component of a broader Internet global ecosystem. The very definition of Internet governance is contested but it is generally referred to as the design and administration of the technologies necessary to keep the Internet operational, as well as the debates around those technologies, such as critical Internet resources, standards, and protocols needed to operate the network. There is an intersection between Internet architecture and content mediation; people's Internet access is cut off (or access restrictions are discussed) to control content sharing and communication. The evolutions in Internet

connectivity, a highly private area mostly under the control of Internet companies and their agreements, raise a number of concerns in terms of stability and censorship. The conference has addressed three main themes.

First, "arrangements of technical architecture are arrangements of power" and "Infrastructure is never just infrastructure," and is also about some understanding of complex technical systems such as the DNS; large-scale debates and mobilization, such as the SOPA and PIPA debates; the technical complexity is often paralleled by the complexity of institutions; and political structures are often embedded technological hybrids. As science and technology studies Susan Leigh Star once said, we need to invert the common sense notion of infrastructure, taking what has often been seen as 'boring' and behind the scenes, bringing it to the floor. Internet governance scholars such as the organizers of this conference, all involved in GigaNet, embrace this perspective in relation to Internet governance.

Second, information technology infrastructure is becoming a proxy for power control, a move that is bound to have a number of unintended consequences. Corporate media producers have lost power over the monetization of their content and are looking to infrastructure as a means of reacquiring that power; some global choke points, despite the Internet's overall decentralization, do exist and the extent to which they are subject to "stress fractures" deserves close consideration. While these control points—some virtual, some material, most often a hybrid of both—do exist, there is often not enough public understanding of how technology works.

Third, the multi-stakeholder discussion often reveals its limits, mostly in contexts of privatization of Internet governance. Much Internet governance is being done through new forms, not governments; examples are regional Internet registries and private telecom companies managing the Internet's backbone. Privatized areas are enacting policies and we are often moving from governments to private sector as Internet governance's crucial actor. From "delegated censorship" to "delegated law enforcement," the spotlight is on private entities.

These three themes raise the question of what are the challenges to the future of Internet governance, and therefore, to Internet freedom. First, there needs to be a focus on issues of interoperability, which is easy to take for granted. In many ways, we have more connectivity than ever. But there is not interoperability between social media platforms, Internet voice software, or cloud computing services in the same way there is in email or web services. For example, Skype, while an excellent application, is based in part on proprietary approaches. There is a shift from an open, unified web in which the publication of open standards has helped foster innovation and compatibility among products to an environment that deprioritizes interoperability and places constraints on interconnection. Constraints on interoperability are constraints on innovation itself.

The DNS is a foundational technical system necessary for the Internet's operation, handling billions of queries per day, and it is increasingly used for content blocking functions for which it was not designed. If DNS query resolution is not universally consistent, this may have serious implications for the universality and stability of the global Internet.

To conclude, the Internet is governed while being in a state of constant flux, and a very complex system; its governance entails issues of both private control and civil liberties; it requires technical design as well as new institutional reforms; this governance is not fixed, anymore than technical architecture is fixed. The consequences of changes to this system should be carefully examined as we move forward.

CONFERENCE SPEAKERS

Introduction: Internet Governance by Infrastructure: The Case of the Domain Name System

Francesca Musiani
Yahoo! Fellow, Institute for the Study of Diplomacy

Panel 1: Enforcement, Security, and Mobilizations: The DNS Today

Moderator

Derrick Cogburn
Associate Professor, School of International Service, American University

Panelists

Steve Crocker
CEO, Shinkuro, Inc. & Chair, ICANN Board

Matthew Schruers
CCIA & Adjunct Professor, Georgetown University

Scott McCormick
Consultant, McCormick ICT International

Luke Pelican
Consultant, Ammori Group

Panel 2: New Actors in Internet Governance: Privatization, Infrastructure, Alternatives

Moderator

Nanette Levinson
Associate Professor, School of International Service, American University

Panelists

Fiona Alexander
Associate Administrator, Office of International Affairs,
National Telecommunications and Information Administration

Matthew Hindman
Associate Professor, George Washington University

Francesca Musiani

Shane Tews
Chief Policy Officer, 463 Communications

Final Keynote: The "Turn to Infrastructure" and the Future of IG

Laura DeNardis
Associate Professor, School of Communication, American University

Georgetown University

Founded in 1789, Georgetown University is a distinctive educational institution—a national university rooted in the Jesuit tradition of social justice and education of the whole person, committed to spiritual inquiry, engaged in the public sphere, and invigorated by cultural pluralism. Georgetown's location in Washington, D.C. provides a unique platform for Georgetown faculty to make their expertise and talents available both to policy institutes in Washington as well as to a wider international audience. No other American university is better positioned to foster a critical dialogue on global issues.

http://www.georgetown.edu

Edmund A. Walsh School of Foreign Service

Georgetown University and the School of Foreign Service exist in the most fertile international arena in the world, allowing the School to establish globally renowned competitive programs and centers as well as offer first class undergraduate and graduate degrees. Founded in 1919, the School remains committed to educating students and preparing them for leadership roles in international affairs.

http://sfs.georgetown.edu

Institute for the Study of Diplomacy

The Institute for the Study of Diplomacy (ISD), founded in 1978, is the School's primary window on the craft of diplomacy. The Institute's constituencies include diplomats, scholars, and Georgetown students. ISD staff and associates teach courses, organize lectures and discussions, mentor students, and participate in university life. The Institute also convenes conferences and working groups, and sponsors and publishes research. ISD international affairs case studies are used in classrooms across the United States and around the world.

http://isd.georgetown.edu

Institute for the Study of Diplomacy
1316 36th Street NW
Washington, DC 20007
Telephone: 202-965-5735