Spam 2005:
Technology, Law and Policy

Center for Democracy & Technology
Washington D.C.

March 2005
# Table of Contents

Introduction

Section 1 - The Problem of Spam

- A Survey Review of the User Experience ................................................................. 5
- Impact of Spam - Humana Business Perspective ...................................................... 9

Section 2 - Technological Responses

- A Multi-Pronged Approach to Eliminating Spam Email and Online Fraud ............... 15
- Spam, Economics and Democracy .......................................................................... 21
- Spam Fighting: Authentication, Accreditation and Reputation ............................... 29
- Identifying Legitimate Email: The Email Accreditation Services of TRUSTe .......... 33

Section 3 - Enforcement of the CAN-SPAM Act

- The CAN-SPAM Act: Overview of Anti-Spam Enforcement in 2004 ....................... 41

Section 4 - Views from Europe

- European Union vs. Spam: A Legal Response ......................................................... 45
- The Experience of the European Union With the “Opt-in” Approach .................... 53

Section 5 - Spam Solutions and Issues of Free Expression and Access to Email

- Non-commercial Email Lists: Collateral Damage in the Fight Against Spam .......... 57
- Human Rights and Spam: A China Case Study ...................................................... 63
The Center for Democracy and Technology is pleased to present this compendium of papers, “Spam 2005: Technology, Law and Policy.”

Passage of the CAN-SPAM Act in late 2003 marked an important milestone in the effort to stem the flow of unwanted, unsolicited commercial email. The law, which went into effect on January 1, 2004, codified minimum requirements for responsible email practices that, coupled with criminal sanctions, were intended to make it possible for law enforcement to identify and prosecute purveyors of spam.

Even as policymakers drafted the legislation, they acknowledged that the CAN-SPAM Act would serve at best as only a partial solution to the spam problem. Indeed, analysts have estimated that in 2004 spam comprised 77% of the messages users found in their email boxes. Strong anti-spam technologies and email users educated about how to avoid online behavior that encourages spammers are also keys to addressing spam.

In recent months, attention has turned to the development of technological measures that lessen the flow of spam closer to its source. While anti-spam measures have traditionally filtered spam at the point of delivery, emerging technologies seek to recognize and stop spam at an earlier point in the email system, alleviating the burden of spam for both recipients and Internet service providers.

These technological developments represent a positive and powerful step forward in the effort to reduce spam, but they also raise fundamental issues about how the Internet should work: To what extent will anti-spam technologies pose barriers to access to this inexpensive medium? On the basis of what criteria will ISPs, assisted by these technologies, decide what email will be delivered? Will anti-spam technologies continue to accommodate anonymous political speech? What will be the impact of these developments on non-profit organizations?

The papers in this compendium attempt to present a snapshot of the current conversation about spam. Some of the papers assess the status of the spam problem and the efforts of law enforcement to use the CAN-SPAM law. Two writers from the European Union offer analysis and perspective about how the problem of spam is addressed through the EU Directive, and why that approach is preferred in Europe. The compendium also includes papers by companies promoting technologies, sometimes coupled with policies and best practices, offering spam solutions to consumers and to businesses. Finally, the compendium offers the perspective of a civil libertarian and a non-governmental organization on the impact of anti-spam efforts on free expression and political speech.

In compiling these papers, we attempted as much as possible to be inclusive and balanced. However, the complexity of the problem and the wide range of solutions under development necessitates that this document is limited in scope. What the compendium does endeavor to do is offer a thoughtful look at the spam problem, efforts to address spam through law both in the US and abroad, and some of the technologies under consideration and the issues they raise.

The result is a compendium that we hope will help to inform the ongoing discussion about how to reduce spam in a manner that best serves consumers, businesses, and ISPs. We hope that it will highlight the importance of addressing this problem in a manner that respects and preserves the vision of the Internet and email as media that promote democratic values and free expression.

We are grateful to the contributors to this compendium and look forward to participating in this inquiry as efforts to reduce spam continue.

Paula J. Bruening
Staff Counsel and Compendium Editor
Regarding Internet security, we use pseudonyms, but the vast majority of Chinese or social classes do not have Internet access. Even though I am [writing] to you, there are thoughts I must keep to myself; there is no opportunity to speak, even briefly, and this is also most regrettable. However, ultimately, one blade of grass can set the prairie ablaze!

--An email received from a Chinese lawyer, who is a reader of Human Rights in China's Chinese weekly e-newsletter, Huaxia Bao.

Addressing spam email via technology and legislation raises key issues of balancing protection of users from unwanted commercial email while protecting their freedom of expression and access to information. These can be seen in the case of China, a leading source of spam mail, one of the most repressive governments, and a major hub for ICT (information and communication technologies) development, representing particular challenges when implementing anti-spam strategies. Even as the Chinese government signs on rhetorically to emerging international norms and encourages the growth of the Internet, it continues to build a sophisticated architecture of censorship and information control that undermines technology as a tool for empowerment. Actions must be analyzed within the realities of local situations to ensure that the crusade to eliminate spam does not aid governments in the repression of their people. With many ICT companies bidding on projects for the 2008 Beijing Olympics and eager to participate in the China boom, HRIC (Human Rights in China) recommends developing “best” business practices, targeted towards different types of IT (information technology) companies and at multiple levels, integrating an international human rights framework into the development and implementation of anti-spam technology and legislation, and ICT infrastructure at large.

Technology and Human Rights

Technology has the potential to serve as a tool for empowering peaceful human rights activism and building a more open and democratic civil society through the free flow of information and online collaboration. More specifically the Internet, including email, can be used to amplify dissident and activist voices; generate global support and attention to critical issues; build a virtual space for citizens to meet and organize; and access shared resources inside and outside of China. Such use of technology empowers China’s human networks, including Chinese non-governmental organizations (NGOs), workers, peasants, students, religious practitioners, intellectuals, democracy activist, journalists, lawyers, AIDS activists and public health advocates. Technology used in collaboration with human rights activism can advance the development of normative standards that the international community has already adopted, such as freedom of expression and access to information, as articulated in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. In addition to signing and ratifying treaties, many governments are also engaged in global norm-setting processes, such as the World Summit on Information Society (WSIS). The WSIS Declaration of Principles includes equitable distribution and access to technology, and protection of indigenous knowledge, culture, and language, in addition to freedom of expression and access to information.


Disproportionate Development and Information Control in China

Even as the Chinese government signs on rhetorically to emerging international norms of inclusiveness, democracy and a "people-centered" vision of an information society and encourages the growth of the Internet, it continues to build a sophisticated architecture of censorship and information control that undermines technology as a tool for empowerment.

The exponential adoption and development of the Internet in China is accompanied by persistent and serious social and economic gaps reflected in a digital divide of gender, economic, geographic and social disparities. In the past seven years, the number of Internet users has grown exponentially from 620,000 to 87 million. The current demographics of Internet users show that 60 per cent of the Chinese Netizen population is made up of young males, and just over half are less than 25 years old. In a country where 364 million young people do not have the opportunity to enroll in secondary education, and where many villages, especially in western China, do not even have sufficient basic infrastructure such as water, power or telephone lines, the potential of the Internet to act as a democratizing force is undermined by uneven access and disparities in economic privilege. As the Human Development Map below shows, along the affluent eastern coast where Beijing, Guangzhou and Shanghai are located, there are significantly higher levels of infrastructure development than in the west, allowing more users to surf the Net from home. Moving away from the financial hubs, a higher percentage of Internet users depend on cyber cafes, which are required by government to use surveillance software.


6. Id.


9. Bu Wei, “The Social Impact of the Internet,” Presentation at the China Digital Freedom conference at University of Cali...
and are under constant threat of closure by authorities. Thus, official crackdowns on Internet cafes have a disproportionate impact on less economically privileged users and those in the least affluent parts of the country.

In addition to these economic and social disparities, a major challenge to building a more open and democratic China is reflected in the People’s Republic of China’s (PRC) control over the flow of information. It uses technical, social and legal approaches within a broader existing legal framework of governing state secrets and state security. Firewalls, proxy servers, filtration software for Internet Service Providers and Internet cafes, email and search engine filtration, Web site blocking and surveillance of Internet cates are among the technical approaches that the Chinese government implements to impede the flow of availability of information to Chinese citizens.\(^\text{10}\) In conjunction with filtering, blocking, and surveillance, social methods, such as mass media, ideology and propaganda are used to control the flow of information and social order at large.\(^\text{11}\) More than 60 laws govern Internet activities in China, including self-censorship regulations to which over 120 Chinese and international companies have agreed to abide. With over 30,000 state security employees monitoring Web sites, chat rooms, and emails, the PRC executes a very effective police apparatus. Currently, over 60 Internet users are in detention for publishing “subversive” content online, including calling for political reform and the free flow of information.

These technical, social and legal techniques to control freedom of expression and access to information function within a broader, sophisticated and complex framework of national security, state secrets and criminal law. The law defines states secrets as “matters that affect the security and interests of the state…” with information that can be classified retroactively and based on consequences.\(^\text{12}\) These methods are not new culturally or historically, but the Internet and new technologies have provided a technological upgrade for the police state. As a result, China’s information control has resulted in censorship and self-censorship; a culture and climate of fear; and an undermined capacity to deal with problems.

### Duality Concerns for Anti-Spam Approaches in China

Addressing spam mail via anti-spam technology and legislation raises key issues of balancing protection of users from unwanted commercial email, while protecting their freedom of expression and access to information. Spam, defined as unsolicited commercial email, currently floods 60 per cent of email traffic, posing a significant global problem. Unwanted email presents security and privacy risks, and costs businesses and organizations time and money. To address these problems, governments, multinational corporations, consumer protection groups and others have developed a “cocktail” approach to stemming the flow of spam, using technology, industry best practices, enforcement through legislation, and consumer education measures.\(^\text{13}\) The CAN-SPAM Act of 2003 was enacted by the US to regulate spam email, imposing limitations and penalties on violators of the Act. In particular, the Act directs the Federal Trade Commission (FTC) to cooperate with foreign states to minimize the dissemination of unwanted emails.\(^\text{14}\)

Information technology and digital communications as tools for empowering human rights activism may be hampered by overbroad anti-spam technology and legislation. The over-breadth and vagueness of the definition and implementation of anti-spam technology may have unintended consequences of blocking freedom of expression. New requirements that email senders identify themselves may undermine protections of anonymity and privacy. The duality\(^\text{15}\) of the technology tools raises concerns for a country with an authoritarian government. The tools used to send non-commercial bulk emails, such as domain spoofing and word obscuring, are often deployed by

---


15. “Dual use technology” is generally used to define technology that has both military utility and sufficient commercial potential to support a viable industrial base. In this case study, HRIC uses this term to refer to technology that can be used to protect users from spam mail, but also be deployed by repressive governments to control information flow.
activists to avoid detection in face of a government architecture of surveillance and censorship. On the other hand the same email filtering tools that block obscene or commercial content, with nothing more than a change in settings, is used by governments to block "subversive" content. Technological methodology to track down individual spammers can also be used to identify the anonymous author of an email critical of government policies. Legislative solutions should recognize this duality in the use of new technologies. Currently the CAN-SPAM Act includes no explicit safeguards regarding the exchange of information across borders and between governments; this lack of transparency regarding the repercussions of technical assistance to repressive governments is also an issue that arises from the current framework to address spam mail. There is currently no mechanism in pace for citizens to monitor the actions of their government under the Act and raise concerns over potential repercussions to freedom of expression or access to information. Time and money spent to protect individuals and non-profits from overbroad anti-spam technology may create higher costs to entry for non-governmental organizations and compromise the democracy-enhancing character of the otherwise inexpensive Internet/email medium.

Addressing Spam in China

As a leading source of spam email, a country with one of the most repressive governments, and a major hub for ICT development, China raises particular challenges when implementing anti-spam technology and legislation. China sends the highest percentage of spam email in comparison to the amount of “good” email sent. (The US sends between 50 to 55 percent spam email; and close to 60 percent “good” mail.) In defense of China’s spam mail problem, the PRC Ministry of Information Industry claims that foreign spammers were utilizing Chinese computers to send spam in order to avoid punishment under their own country’s law. As a result, the PRC is asking for more cooperation with other countries in law enforcement to control spam and more assistance from international companies on network security to strengthen anti-spam technology, which raise questions of transparency and the consequences of information sharing across borders.

With the highest number of Internet activists imprisoned and a sophisticated architecture of surveillance and censorship, the PRC is also one of the leading countries in information control. Because anti-spam technology works similarly to filtering and censorship measures that the PRC currently deploys, anti-spam technology and legislation may legitimize China’s position to further control and repress the flow of information – both within China, and in and of China. Anti-spam tools may also provide the government with greater ability to track people’s actions on the Internet, violating privacy and security rights, and leading to increased self-censorship and more arbitrary arrests and detentions. The intersection of China’s state secrets and state security legislation and the over-breadth and vagueness of anti-spam legislation and technology could provide more tools for the PRC government to chill freedom of expression and foster a climate of fear.

Getting a ‘Piece of the Action’

China’s booming IT market and its hosting of the 2008 Beijing Olympics are attracting high profile ICT companies to get a “piece of the action.” Yet the 2002 self-censorship pledge and recent issues with Google’s search engine in China raise questions about the role of companies – both international and domestic – doing work in China. In March 2002, the Internet Society of China asked international and Chinese companies to “volunteer” signing on to a self-censorship pledge, in which companies agreed to refrain from posting information that will “jeopardize state security and disrupt social stability” among other restrictions. A few months ago and still ongo-


ing, studies by the Open Net Initiative\textsuperscript{22} and Dynamic Internet Technology, Inc.\textsuperscript{23} on Google’s search engine in China show that the Chinese government is filtering search results and keywords. With existing Internet companies already being compromised of filtering their search engines, what are the implications of deploying anti-spam technology in China? How can companies, governments, consumers and NGOs ensure that technology built for China is not also implemented or modified for repressive purposes?

With many ICT companies bidding on projects for the Olympics and eager to participate in the China boom, HRIC recommends developing “best” business practices, targeted towards different types of IT companies and at multiple levels. The circuit tree below describes the path a user request travels, identifying key transactions. Every request routed through the network passes multiple points at which concerns exist for censorship or the invasion of privacy. Starting at the desktop level, Internet cafés and many companies are required to install filtration and surveillance software. At the ISP level it is possible to capture user requests and search for specific terms and data. When the request moves out into the Internet backbone it must pass through the “Great Firewall.” Finally, at the destination server information can be collected based both on automated Web logging as well as data requested or offered by the users. Each level is distinct and although the basic concerns stay the same, different mechanisms are needed to protect them based on the technical details of each. Additionally, we have identified examples of some companies carrying the traffic at each level.

Based on the circuit tree below we have outlined a possible framework for exploring best practices that should be developed with the input and participation of multiple stakeholders, including NGOs, consumers, and business. The matrix focuses on three types of IT companies: information providers, hardware and software developers, and connectivity. Mapped to each of type of company are the backbone, Internet Service Provider, and end user levels. The matrix

\begin{figure}
\centering
\includegraphics[width=\textwidth]{chart1.png}
\caption{Communication Path}
\end{figure}

Source: Human Rights in China with contribution from Michael To


reflects a preliminary model for developing best practices that address both domestic implementation and cross-border impact of anti-spam technology and legislation with regards to censorship and freedom of expression; privacy and anonymity; and surveillance and security issues. For each area of concern, the framework identifies some specific issues to consider in developing best practices.

Chart 2: IT Best Practices Matrix
Integrating an International Regulatory Framework

China illustrates the dangers of cross-border implementation, on legal, technical, and policy levels, of anti-spam technology and legislation. To address these challenges, HRIC urges policy interventions at multiple levels, integrating an international human rights framework into the development and implementation of anti-spam technology and legislation, and ICT infrastructure at large. An international regulatory framework that can be applied across borders will prevent adverse consequences in other regions. To govern an increasingly global Internet, transparency and accountability for both multinational corporations and governments are critical to properly monitor the modification and implementation of technology. In addition, careful and independent monitoring will ensure that freedom of expression and access to information on the Internet are protected, and that all stakeholders are included in a meaningful way in the design and implementation of the future Internet, both in policy-making and in engineering.