Relatório para a Comissão de Trabalho sobre Spam do Comitê Gestor da Internet no Brasil:

Análise Técnica de Algumas Legislações sobre Spam

Cristine Hoepers Klaus Steding-Jessen
Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil – CERT.br

19 de agosto de 2005

Resumo

Este documento apresenta uma análise dos aspectos tecnológicos de 4 legislações internacionais sobre spam consideradas pertinentes, de 7 projetos de lei nacionais de conhecimento dos autores e do Código de Ética AntiSPAM. São também apresentadas considerações técnicas sobre a efetividade de muitos dos mecanismos discutidos.

Sumário

Lista de Tabelas

1 Introdução

Este documento não é uma análise jurídica sobre legislações anti-spam, assim como não é exaustivo. Ele apresenta uma análise sobre os aspectos tecnológicos de algumas legislações internacionais sobre spam, bem como estes aspectos nos projetos de lei nacionais de conhecimento dos autores.

Serão descritos alguns pontos comumente presentes em diversas legislações sobre spam, como a definição de qual conteúdo é proibido e quais regras devem ser seguidas.

Após as definições destes pontos é apresentada uma tabela comparativa das leis e projetos de lei analisados, levando-se em conta os pontos descritos.

Por fim, os autores apresentam considerações técnicas sobre a efetividade de muitos dos mecanismos propostos e recomendam pontos que devem estar presentes em uma possível lei contra spam.

2 Pontos Normalmente Abordados em Legislações Anti-Spam

Nesta seção serão apresentados, com ênfase na parte técnica, diversos pontos que normalmente estão presentes em muitas das legislações atuais ou projetos de lei.

2.1 Regra para Contato: *Opt-in* × *Opt-out*

De maneira genérica, pode-se dizer que as legislações anti-spam adotam um dos dois seguintes tipos de regras para contato com o destinatário:

- é proibido mandar mensagens comerciais/spam, a menos que exista uma concordância prévia por parte do destinatário (*opt-in*);
- é permitido mandar mensagens comerciais/spam, mas deve-se prover um mecanismo para que o destinatário possa parar de receber as correspondências (*opt-out*).

Existem algumas leis que propõem as seguintes variantes:

- *Soft Opt-in* – neste caso há uma exceção quando já existe uma relação comercial entre remetente e destinatário, de forma que não seria necessária a permissão explícita por parte do destinatário;
- permissão para o primeiro *e-mail* – muitas leis e projetos de lei colocam que é permitido um primeiro *e-mail*, sendo vedada a repetição de *e-mails* similares posteriores.

2.2 Identificação da Mensagem

Algumas das leis propõem que as mensagens comerciais/spam contenham uma identificação distinta, que facilite a sua identificação e possível filtragem. Em alguns casos esta identificação seria no assunto da mensagens, em outros no cabeçalho ou no primeiro parágrafo.

Exemplos são: "`@`" e "ADLT", adotadas pela Coréia do Sul; "ADV", adotada por alguns estados dos EUA; e "PUBL", citada em um dos projetos de lei nacionais.

2.3 Assunto Enganoso

Alguns textos colocam que uma mensagem pode ser considerada spam se o seu assunto for enganoso, ou seja, se induzir o destinatário a interpretar erroneamente a natureza, contexto ou conteúdo da mensagem.

Por exemplo, um assunto como "Re: solicitação", que pode levar o destinatário a pensar que se trata de uma resposta a um *e-mail* seu.

2.4 Informações Falsas

Algumas leis proíbem expressamente a falsificação de informações como identidade, dados de contato, domínios, cabeçalhos, data, hora, além da inclusão de subterfúgios que dificultem ou impossibilitem o bloqueio automático de mensagens.

2.5 Identificação do Remetente

Diversas leis exigem que o remetente das mensagens forneça informações corretas sobre sua identidade, endereço de correspondência e endereço eletrônico.

2.6 Aquisição dos Dados

Algumas leis internacionais abordam a questão da origem e da forma como os dados usados para o envio das mensagens foram obtidos. Elas proíbem a utilização de dados obtidos através de técnicas de *harvesting* ou ataques de dicionários.

Alguns projetos de lei nacionais determinam que o remetente deve explicitar em sua mensagem a origem dos dados do destinatário.

2.7 Requerimentos de Remoção

Existem em diversas leis requerimentos para que seja prevista a remoção dos dados do destinatário das bases de dados dos remetentes. Este requerimento é aplicável tanto para leis cujas regras de contato sejam *opt-in*, quanto para aquelas que sejam *opt-out*.

2.8 Mídias

A maior parte das leis e projetos define a quais mídias se aplica a lei/projeto em questão. É comum encontrar referências a mensagem eletrônica, *e-mail*, VoIP, IM, SMS/MMS, fax, telefone, etc.

3 Análise de Leis Internacionais

Nesta seção será apresentada uma tabela comparativa das legislações dos seguintes países:

Estados Unidos: CAN-SPAM Act of 2003 – http://www.spamlaws.com/federal/108s877.shtml

Austrália: SPAM ACT 2003 – http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm

União Européia: European Union Directive 2002/58/EC on Privacy and Electronic communications – http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

Coréia do Sul Article 50 of the "Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection" of 2001 – http://www.bakercyberlawcentre.org/2003/Privacy_Conf/papers/Day2/Chung_spam.doc

País	Opt in	Opt out	Identificação da Mensagem	Assunto Enganoso	Informações Falsas	Identificação do Remetente	Aquisição dos Dados	Requerimentos de Remoção	Mídias	Observações
EUA CAN-SPAM Act of 2003		✔	prevê o uso de identificadores, mas ainda não foram definidos	sim	proíbe domínios e cabeçalhos com dados falsos	• endereço de retorno válido • endereço de correspondência	• proíbe *harvesting* e ataques de dicionário • só é considerado *harvesting* se o site tiver um *disclaimer* contra	por *e-mail* ou outra forma baseada em Internet	*e-mail*	• assume que remetente é uma pessoa • deixa claro que é comercial se não houve consentimento prévio • são agravantes: *harvesting*, ataque de dicionário, uso de relay/proxy abertos • permite que um endereço de retorno de uma mensagem acuse um "erro temporário" por um tempo indefinido
Austrália	✔					as informações devem ser corretas	proíbe *harvesting*	método funcional de remoção	• *e-mail* • IM • VoIP • similares	• deve haver uma relação do spam com a Austrália • proíbe produção, uso e venda de softwares de *harvesting* • é irrelevante se os produtos anunciados existem ou não
EU Diretriz 2002/58/EC	✔				proíbe identidade falsa	• identidade do remetente • endereço de retorno válido		deve haver algum método de remoção	• *e-mail* • fax • SMS/MMS • *calling machines*	• "soft opt-in" e para empresas existe a opção de opt-out • não há restrição contra *harvesting*
Coréia do Sul		✔	• ADV • ADLT • proíbe identificadores "irregulares"		cabeçalho deve estar correto	informações corretas de contato	• proíbe *harvesting* e ataques de dicionário • só é considerado *harvesting* se o site tiver um *disclaimer* contra • proibido compartilhar listas de *e-mail*		• *e-mail* • fax • telefone • novas mídias, por decreto	• proibido relay aberto • proibição de ataques de dicionários para telefones • ISPs podem negar serviço para spammers

Tabela 1: Tabela de Leis Internacionais Analisadas

4 Análise de Projetos de Lei Nacionais

Nesta seção é apresentada uma comparação entre 7 projetos de lei tramitando no Congresso Nacional, incluindo uma comparação destes com o Código de Ética AntiSPAM. Os textos analisados foram:

Código de Ética AntiSPAM e Melhores Práticas de Uso de Mensagens Eletrônicas: http://brasilantispam.org/main/codigo.htm

PL 2186/03 de autoria de Ronaldo Vasconcellos

PL 2423/03 de autoria de Chico da Princesa

PL 3731/04 de autoria de Takayama

PL 3872/04 de autoria de Eduardo Paes

Substitutivo ao PL 2186/03 relator: Nelson Proença – apensados os projetos 2423/03, 3731/04 e 3872/04.

PLS 367/2003 de autoria de Hélio Costa

PLS 21/2004 de autoria de Duciomar Costa

PLS 36/2004 de autoria de Antonio Carlos Valadares

Os textos dos projetos de lei foram retirados dos sites da Câmara dos Deputados e do Senado Federal.

País	Opt in	Opt out	Identificação da Mensagem	Assunto Enganoso	Informações Falsas	Identificação do Remetente	Aquisição dos Dados	Requerimentos de Remoção	Mídias	Observações
Código de Ética AntiSPAM		✔	NS (*)	proíbe tema diferente do conteúdo (*)	proíbe identificação falsa do remetente	deve haver identificação (*)	permite coleta via formulários em sites e/ou *e-mails*, explicitando a finalidade	deve haver uma maneira de remoção (*)	• correio eletrônico • telefone celular • Internet • IM	• é opt-out porque assume que é possível enviar um *e-mail* com uma opção de opt-in, além de o opt-in ser opcional • (*) só é considerado spam quando dois ou mais destes requisitos forem infringidos
PL 2186/03 Ronaldo Vasconcellos		✔	cabeçalho, assunto e primeiro parágrafo com identificação clara		proíbe o uso de endereços de terceiros	informação válida e confirmável			*e-mail*	• é preciso optar para receber os demais • artigo sexto não é claro • contraditória: se diz opt-in, mas permite o primeiro *e-mail*
PL 2423/03 Chico da Princesa		✔	cabeçalho e primeiro parágrafo com identificação clara			identificação e *e-mail*				• originado/destinado para o Brasil • contraditória: se diz opt-in, mas permite o primeiro *e-mail* • sugere filtragem de mensagens pelos ISPs
PL 3731/04 Takayama		✔	cabeçalho e/ou primeiro parágrafo com identificação clara			identificação e *e-mail*			mensagem eletrônica	• contraditória: opt-out, mas após o primeiro *e-mail* o usuário deve autorizar os demais • usuário tem o direito de bloquear mensagens • filtragem por origem pelos ISPs num prazo de 72h
PL 3872/04 Eduardo Paes		✔			proíbe falsear ou fraudar informações do remetente, data/hora ou roteamento da mensagem				*e-mail* ou "outro procedimento"	• define mensagem não identificada • item 5 troca remetente com destinatário • define relação comercial pré-existente

Tabela 2: Tabela dos Projetos de Lei Nacionais Analisados

País	Opt in	Opt out	Identificação da Mensagem	Assunto Enganoso	Informações Falsas	Identificação do Remetente	Aquisição dos Dados	Requerimentos de Remoção	Mídias	Observações
Substitutivo ao PL 2186/03	✔								mensagem eletrônica por computador	• "soft" opt-in • cria cadastro de opt-in, mantido pelo provedor • define que o provedor deve fornecer, gratuitamente, software antivírus aos usuários • apensados os projetos 2423/03, 3731/04 e 3872/04
PLS 367/2003 Hélio Costa		✔				nome e endereço			*e-mail*	• originado/destinado ao Brasil • permite o primeiro *e-mail* • filtragem por origem pelos ISPs num prazo de 24h
PLS 21/2004 Duciomar Costa	✔		PUBL e PUBL:ADULTO		proíbe meios que impeçam ou dificultem bloqueio automático	endereço físico, IP e URL	deve explicitar a origem dos dados	mecanismo eficaz, claro, compreensivel, simples e gratuito	texto, voz, som ou imagem enviados pela Internet	• mensagem comercial só se for para mais de 500 destinatários em 96h • parágrafo 2 possibilita *spamvertised website* • uso de *cookies* ou outros mecanismos de rastreamento devem ser explicitados e evitáveis • o usuário tem direito a usar filtros • estimula recompensa ao dar 20% da multa ao denunciante • impede compartilhamento da base de dados
PLS 36/2004 Antonio Carlos Valadares		✔	Publ e Publ:Adulto		não pode esconder ou falsear endereços de origem ou informações mínimas de identificação do remetente e do propósito		deve indicar a base de dados usada	devem haver mecanismos para optar pelo não recebimento	mensagens eletrônicas	• permite a primeira mensagem • usuário tem o direito de bloqueio • ISPs não podem fornecer base de *e-mails* a terceiros • cria cadastro nacional público de usuários que não desejam spam

Tabela 3: Tabela dos Projetos de Lei Nacionais Analisados (cont)

5 Considerações sobre a Efetividade dos Pontos Abordados nas Leis e Projetos Analisados

Nesta seção serão feitas algumas considerações sobre a efetividade e necessidade de cada um dos pontos utilizados na comparação entre as leis e projetos de lei.

5.1 Regra para Contato: *Opt-in* × *Opt-out*

Embora a maioria dos textos analisados adote *opt-out* como opção de regra de contato, utilizar *opt-out* abre uma brecha para que todos os spams sejam enviados e estejam de acordo com a lei.

O *opt-out* coloca sobre o destinatário o ônus de ter que se desinscrever de um número enorme de fontes propaganda, quando provavelmente ele gostaria de receber mensagens apenas de um número várias ordens de grandeza menor. Não é lógico pensar que deve ser responsabilidade do usuário dizer de quem ele não deseja receber mensagens, especialmente em função do número de mensagens envolvidas, quando é muito mais natural que parta do usuário a iniciativa de escolher as fontes de propaganda que deseja receber (*opt-in*).

Na tentativa de reduzir o volume de *e-mails* recebidos se adotado o *opt-out*, alguns projetos propõe a idéia de permitir somente o primeiro *e-mail*. Porém, tecnicamente é possível que uma pessoa envie diversas vezes o mesmo conteúdo em mensagens que poderão sempre ser consideradas a primeira mensagem. Isto é possível se o remetente a cada vez utilizar um endereço de retorno diferente, um servidor diferente para enviar a mensagem, alterar a URL onde está o conteúdo anunciado, etc.

Além disso, ao definir que a maneira como a pessoa possa sair de uma lista de *e-mails* de um spammer seja entrando em contato com ele, vai contra todas as recomendações de boas práticas. Ao responder a um spam solicitando para sair, normalmente o destinatário está apenas confirmando que seu *e-mail* é válido. Se o esquema de remoção for através de um link no *e-mail*, isto abre brechas para um novo vetor de disseminação de ataques de phishing/scam.

Recomenda-se, então, que a melhor opção para regra de contato é o *opt-in* ou até mesmo o *soft opt-in*, que considera legal o envio de mensagens para destinatários com os quais o remetente já possui uma relação comercial prévia.

5.2 Identificação da Mensagem

A adoção de identificadores como "`@`", "ADLT", "ADV" ou "PUBL" foi concebida para, em teoria, ajudar o usuário a identificar facilmente mensagens não solicitadas. Porém, para que isto pudesse atingir o objetivo proposto, seria necessário que todos aqueles que enviam mensagens não solicitadas assumissem que o estão fazendo e seguissem a regra – o que normalmente não é o caso.

Sabe-se da existência de programas para envio de spam que já possuem opções de configuração para colocar identificações nas mensagens e tornar o spam de acordo com a lei.

Outra dificuldade deste método é a multiplicidade de padrões propostos, que ao final tornaria inviável para uma mensagem legítima de contato de uma empresa com um cliente ficar de acordo com todas as diferentes exigências. Além disso, a inclusão de múltiplos identificadores no campo assunto dificulta para os destinatários a identificação do conteúdo da mensagem.

Em função de todos estes problemas, já é consenso da comunidade técnica que, além de ser ineficaz, a utilização de identificadores de mensagens é prejudicial para o sistema de correio eletrônico, vide os documentos [1, 2].

5.3 Assunto Enganoso

Algumas leis internacionais proíbem a utilização de assuntos enganosos, de forma a poder penalizar *e-mails* como os phishing/scams ou outras que tentem induzir o usuário a erro. Este ponto parece ser interessante, inclusive como um agravante para os casos em que as mensagens recebidas façam parte de esquemas fraudulentos.

5.4 Informações Falsas

Como o objetivo da inclusão de informações falsas de domínio, data, hora, cabeçalhos e identidade normalmente é dificultar que seja possível identificar o remetente da mensagem, explicitar que este subterfúgio é proibido é bastante interessante.

5.5 Identificação do Remetente

Apesar da exigência de identificação do remetente se sobrepor com a proibição de usar dados falsos, muitos projetos e leis explicitam exatamente quais informações sobre o remetente devem ser incluídas na mensagem. Isto é interessante, pois ajuda o destinatário a saber exatamente quem é a empresa/pessoa que está entrando em contato com ele.

5.6 Aquisição dos Dados

Seria bastante interessante que os projetos de lei nacionais, a exemplo de algumas leis internacionais, incluíssem artigos que abordassem quais são as maneiras ilegais de obter dados e quais seriam alternativas legais.

É muito relevante, por exemplo, a proibição da produção de programas que realizem *harvesting*, bem como a comercialização e o uso deste tipo de programa e dos dados através dele obtidos, presente na lei Australiana.

A obtenção de dados através de *harvesting* tem sido a maior fonte de endereços de *e-mail* para os spammers, sendo que hoje o *harvesting* é feito não somente em páginas web, mas também por meio de códigos maliciosos instalados sem conhecimento/consentimento dos usuários, como cavalos de tróia, vírus, *worms* e *bots*. Adicionalmente, seria interessante que fosse proibida a utilização de ataques de dicionário para formação de bases de *e-mails*.

É muito importante que a proibição da produção e uso destas técnicas seja completa, sem a necessidade de páginas web conterem *disclaimers* sobre a proibição de uso.

5.7 Requerimentos de Remoção

É importante que um destinatário tenha o direito de ser removido de uma lista a qualquer tempo – mesmo que ele tenha optado por receber as mensagens. O ideal é que seja algum mecanismo que não induza o destinatário a seguir um *link* presente em uma mensagem.

5.8 Mídias

Atualmente a forma mais popular de spam ocorre por *e-mail*, porém há uma tendência cada vez maior da ocorrência de spam em outros meios, como sistemas de mensagens instantâneas (IM), telefones celulares (SMS/MMS), voz sobre IP, telefonia convencional (fax e mensagens gravadas), etc.

É importante que uma lei possua uma definição ampla o suficiente do meio em que o spam possa ocorrer, para permitir que sejam cobertas pela lei novas mídias que possam ser utilizadas para o envio de spam.

5.9 Outros Pontos Relevantes

Alguns projetos incluem artigos preocupantes, que embora não se enquadrem nos pontos discutidos anteriormente, podem abrir brechas para legalizar o spam e também facilitar a obtenção de endereços de *e-mail* por parte de spammers.

Um dos projetos propõe que só pode ser considerada spam a mensagem que for enviada para mais de 500 pessoas num prazo de 96 horas. Isto permite a adaptação dos programas de envio spam para se adequar a este limite, possivelmente combinando múltiplos remetentes para atingir um número maior de mensagens enviadas.

Outro projeto propõe a criação de um cadastro nacional com todos os endereços daqueles que não desejam receber spam. Isto é preocupante, não só do ponto de vista de privacidade, mas também porque manterá públicos endereços de pessoas que não querem receber mensagens, possibilitando a captura de seus *e-mails* por programas de *harvesting*.

6 Conclusões

O maior desafio para uma lei anti-spam é que ela não legitime o spam, ou seja, que não permita o envio de um spam que possa estar de acordo com a lei. Um exemplo disso é o CAN-SPAM Act de 2003, dos Estados Unidos, onde o número de spams enviados e que estavam de acordo com a lei dobrou de outubro para novembro de 2004 [3].

Todas as leis que adotaram um esquema *opt-out* enfrentam ou correm o risco de enfrentar o problema de legitimar os spams.

A única maneira que parece viável para criar uma lei que não legitime o spam é a adoção de um sistema estritamente *opt-in*, ou seja:

- que não permita o primeiro *e-mail*;
- que não permita convites por *e-mail*.

Neste caso existe uma iniciativa por parte do destinatário de receber uma mensagem de conteúdo comercial. Uma possível atenuação seria a adoção de um esquema *soft opt-in*, que tem como exceção o envio de mensagens para destinatários com os quais o remetente já possui uma relação comercial prévia.

Outro fator polêmico é a adoção ou não de identificadores de mensagens. Os estudos mostram que estes identificadores não são eficazes e podem ser prejudiciais para o sistema de correio eletrônico, não sendo recomendada sua inclusão em uma lei anti-spam [1, 2].

É importante que uma lei aborde quais são as maneiras ilegais de obter dados e possua uma definição ampla o suficiente do meio em que o spam possa ocorrer, para cobrir novas mídias que possam ser utilizadas para o envio de spam.

Glossário

Ataque de dicionário
: Na literatura de spam, um ataque de dicionário consiste em formar endereços de *e-mail* a partir de palavras constantes em dicionários e/ou da combinação de caracteres alfanuméricos.

Bot
: Programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar spam, etc.

Cavalo de Tróia
: Programa, normalmente recebido como um presente (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem conhecimento do usuário.

Código Malicioso
: Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de tróia, etc.

Harvesting
: Técnica utilizada por spammers, que consiste em varrer páginas web, newsgroups, arquivos de listas de discussão, entre outros, em busca de endereços de *e-mail*.

IM
: *Instant Messaging*.

MMS
: *Multimedia Messaging Service*.

Phishing
: Também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Proxy
: Um servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. Proxies mal configurados podem ser abusados por atacantes e utilizados como uma forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar spam.

***Relay* Aberto**
: Servidor de *e-mail* mal configurado, permitindo que seja usado para enviar mensagens de/para qualquer rede ou domínio, independente dos endereços envolvidos serem da sua rede ou não.

SMS
: *Short Message Service*.

Spam
: Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês *Unsolicited Commercial Email*).

Spammer
: Pessoa que envia spam.

Vírus
: Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

VoIP Voz sobre IP, do inglês *Voice over IP*.

Vulnerabilidade
Falha no projeto, implementação ou configuração de um software ou sistema operacional, que quando explorada por um atacante resulta na violação da segurança de um computador.

Worm Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros progamas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

Referências

[1] C. Malamud, "RFC 4096: Policy-Mandated Labels Such as "Adv:" in Email Subject Headers Considered Ineffective At Best." http://www.ietf.org/rfc/rfc4096.txt, May 2005.

[2] D. P. Majoras, O. Swindle, T. B. Leary, P. J. Harbour, and J. Leibowitz, "Subject Line Labeling As a Weapon Against Spam: A CAN-SPAM Act Report to Congress," tech. rep., Federal Trade Commission, June 2005. http://www.ftc.gov/reports/canspam05/050616canspamrpt.pdf.

[3] R. Kolstad, "The Only Good Spam Comes from Hormel," *;login:*, vol. 30, pp. 2–3, February 2005. http://www.usenix.org/publications/login/2005-02/openpdfs/motd.pdf.

[4] "The European Coalition Against Unsolicited Commercial Email." http://www.euro.cauce.org/en/index.html.

[5] M. C. Bueti, "ITU Survey on Anti-Spam Legislation Worldwide," Tech. Rep. CYB/06, International Telecommunication Union, 2005. http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[6] D. E. Bambauer, J. G. P. Jr., and D. E. Abrams, "A Comparative Analysis of Spam Laws: the Quest for Model Law," Tech. Rep. CYB/03 Prov., International Telecommunication Union, June 2005. http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf.

[7] M. B. Prince, "Countering Spam: How to Craft an Effective Anti-Spam Law." http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf, 2004.

[8] "Federal Trade Commission Spam Website." http://www.ftc.gov/bcp/conline/edcams/spam/index.html.