

## Spam and Internet Privacy

By: B.G. Kutais

New York: Novinka Books, 2007, ISBN: 978-1-59454-5771-1

Price \$39.00, pp.129

Reviewed by: Michael B. Forte, Jr.

Journal of High Technology Law

Suffolk University Law School

---

As the prevalence of email use has gained popularity, the burden that junk email incurs has greatly increased.<sup>1</sup> The problems that spam can cause result in more than just mere annoyance. Spam can: drive people away from the use of email because it can undermine user trust of email, reduce firm productivity when it clogs business email boxes, and increase costs for internet service providers which will eventually be passed down to the consumer.<sup>2</sup> In *Spam and Internet Privacy*, Editor B.G. Kurtais compiles a number of pieces in an effort to demonstrate how the “boiling issues”<sup>3</sup> of spam and internet based invasions of privacy are being addressed by the law and by Congress. Kutais chooses including excerpts from Congressional Research Service Reports and a copy of the CAN-SPAM Act of 2003.<sup>4</sup> This book presents a balanced view of the debate regarding specific legislative actions that were contemplated earlier in the decade. That said, in some of the excerpts the author makes unsupported assertions that do not seem to be in line with the concerns many Americans have regarding technology threats. Overall, this book presents a survey of the state of the law regarding spam and internet privacy

---

<sup>1</sup> See *infra* note 4, CAN-SPAM § 2(a)(1)-(2).

<sup>2</sup> Organization for Economic Co-Operation and Development, *OECD work on Spam*, available at: [http://www.oecd.org/department/0,3355,en\\_2649\\_22555297\\_1\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/department/0,3355,en_2649_22555297_1_1_1_1_1,00.html) (last accessed Sept. 25, 2007).

<sup>3</sup> B.G. KUTAIS, SPAM AND INTERNET PRIVACY, Preface (Novinka Books 2007) (hereinafter “Kutais”).

<sup>4</sup> 15 U.S.C. § 7701, *et seq* (2006) (hereinafter “CAN-SPAM”).

which is useful to the novice wishing to learn about some of the issues presented, but does not work well for more experienced advocates on either side of the debate.

*Spam and Internet Privacy* is Kutais's latest focus on internet policy and use. His previous works including *The Internet Glossary*<sup>5</sup> and *Trends in Internet Research*<sup>6</sup> gave novices an insight into the computer world. In *Spam and Internet Privacy* he attempts to synthesize a coherent framework that will address two related, but distinct topics.

The threats produced by invasions of internet privacy, and spam are difficult to control for several reasons. Spam is a term without a universally recognized definition and addressing the issue of spam will require specific measures that not everyone can agree will benefit email users. Internet privacy threats come in numerous varieties and are changing as technology progresses. Accordingly, the challenge policy makers face is to create laws that will address technologies not yet in existence, while at the same time not restricting legitimate internet use.

The lack of a universally recognized definition for spam is one of the major obstacles to creating solutions designed to minimize its harmful effects. The definition of spam could range from any unsolicited emails,<sup>7</sup> to unsolicited commercial emails sent by any source,<sup>8</sup> to unsolicited commercial emails from sources the recipient has never had contact with,<sup>9</sup> to simply emails or postings transmitted in bulk quantities.<sup>10</sup> Each of these

---

<sup>5</sup> B.G. KUT AIS, THE INTERNET GLOSSARY (Nova Science Pub, Inc. 2002).

<sup>6</sup> B.G. KUT AIS, SPAM AND INTERNET RESEARCH (Nova Science Pub, Inc. 2004).

<sup>7</sup> See [http://www.oecd-antispam.org/article.php3?id\\_article=234](http://www.oecd-antispam.org/article.php3?id_article=234) (last accessed Sept. 30, 2007).

<sup>8</sup> See <http://www.consumerfraudreporting.org/spam.php> (last accessed Sept. 20, 2007).

<sup>9</sup> This would not include prior business relationships or transactional messages and is the preferred definition used by the Federal Trade Commission.

<sup>10</sup> See <http://www.stopspam.org/definitions.html> (last accessed Sept. 20, 2007).

definitions would include emails that are arguably constitutionally protected,<sup>11</sup> or emails that recipients may desire to receive. Accordingly the first challenge is to define spam in such a way that it does not burden legitimate communications. Marketing associations attempted to institute a vision of spam that would allow its members to communicate freely with the public.<sup>12</sup> Privacy advocates wanted a restrictive definition.<sup>13</sup> This fight was not simply a semantic distinction. It would affect the classification of whole groups of communications and the applicability of regulations to their emails.

Once the issue of spam's definition is reconciled, other debates rage that focus on the specific solutions that were proposed to eliminate spam. During the previous three congressional terms some of the proposed solutions introduced included the creation of a do-not-spam email registry,<sup>14</sup> regulation limiting the amount of emails a source could send,<sup>15</sup> and language requiring specific phrases or labeling in the subject lines of emails were proposed as well.<sup>16</sup>

In the end Congress pre-empted several state laws that broadly defined spam and restricted its use.<sup>17</sup> Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.<sup>18</sup> The act prohibited the conveyance of emails: that had deceptive subject lines,<sup>19</sup> that were sent to users who had already "opted-out" of

---

<sup>11</sup> The right of companies to advertise has been recognized as protected speech under the First Amendment. *See* Greater New Orleans Broad. Assoc. v. United States, 527 U.S. 173, 188 (1999).

<sup>12</sup> Direct Marketing Association, Anti-Spam Working Strategy, available at <http://www.the-dma.org/cgi/disppressrelease?article=452> (last accessed Sept. 30, 2007).

<sup>13</sup> *See infra* note 24.

<sup>14</sup> S. 563, 108<sup>th</sup> Cong.

<sup>15</sup> CAN-SPAM § 4(b)(2)(C).

<sup>16</sup> CAN-SPAM § 5(d).

<sup>17</sup> *See* <http://www.spamlaws.com> (last accessed Sept 30, 2007).

<sup>18</sup> *See supra* note 3.

<sup>19</sup> CAN-SPAM § 5(a)(2).

receiving emails from the source,<sup>20</sup> that displayed pornographic subjects without warning,<sup>21</sup> that were fraudulent,<sup>22</sup> or that harvested information about the user.<sup>23</sup> By allowing for opting-out marketers were allowed to send messages and privacy advocates were dismayed.<sup>24</sup> The Federal Trade Commission was also given rulemaking authority to recommend whether bounty systems or do-not-email registries were feasible.<sup>25</sup>

Privacy can be treated as a different subject from spam. Threats to one's privacy emerge in various forms on the internet. Some are overt and immediately recognizable to their victims. Others lay in the system of the user's computer and may never be discovered, but can nonetheless harm the user. New forms of invasion such as phishing, spyware, identity theft or fraud, the monitoring of the content of communications, and the tracing browsing history and internet transactions constantly threaten internet users. Several pieces of legislation have been introduced in both Washington and state capitals to deal with these ever changing threats. But the law's ability to keep up with the technological advances that threaten privacy has created opportunities for both governmental and criminal forces to take advantage of the average citizen's internet activities.

Kutais's attempt to synthesize a coherent framework for such a dynamic and wide field succeeds in providing the novice a useful resource. Kutais chooses pieces which present a brief explanation of the issues with which Congress dealt, the viewpoints on

---

<sup>20</sup> CAN-SPAM § 5(a)(4).

<sup>21</sup> CAN-SPAM § 5(d).

<sup>22</sup> CAN-SPAM § 5(a)(1).

<sup>23</sup> CAN-SPAM § 5(b).

<sup>24</sup> Coalition Against Unsolicited Commercial Email, CAUCE Statement On CAN SPAM Act, <http://www.cauce.org/archives/26-CAUCE-Statement-on-CAN-SPAM-Act.html> (last accessed Sept. 30, 2007).

<sup>25</sup> A CAN-SPAM Informant Reward System, available at <http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf> (last accessed Sept. 30, 2007).

each side of the debate of each issue, and several bills Congress members introduced to solve the problems. This approach gives a thorough historical prospective of the debate, but lends little to the current state of the law in a dynamic field. Accordingly, the book is not a good reference for an advocate or expert involved in litigation. However, the book is a good fit for the lay reader, or the inexperienced computer user who seeks to learn the background and policy debates surrounding spam and internet privacy laws.

Each of the five chapters deal with a specific subject. Spam topics are covered in the first three chapters. Chapter four is an analysis of internet privacy threats and pieces of legislation designed to address those threats. Chapter five provides a copy of the CAN-SPAM Act. The author also notes that the spam issue can be treated as a privacy issue. The emphasis on spam might lead one to believe that it is possibly a more pressing issue than internet privacy in general, but in the time since these reports were written internet privacy has become a much greater concern.<sup>26</sup>

Kutais's description of the issues as "boiling" is accurate in some respects. The basic issues that are presented have not gone stale. Concerns over internet privacy have only increased as the war on terror has continued and as incidents of identity theft have increased. Spam still fills email boxes and presents email service providers with the challenge of implementing systems to fight it.

There is one lacking aspect in the book and an opinion which goes unsupported. To address many of the internet privacy concerns Kutais chose to include a Congressional Research Service Report that purports to "discuss Internet privacy issues

---

<sup>26</sup> *Identity Theft: Innovative Solutions for an Evolving Problem* Before the Subcomm. on Terrorism, Technology, and Homeland Security of the S. Comm. on the Judiciary, 110<sup>th</sup> Cong. 3 (March 21, 2007) (statement of Lydia Parnes, Director of the Bureau of Consumer Protection at the Federal Trade Commission) (available at: <http://www.ftc.gov/os/testimony/P065409identitytheftsenate03212007.pdf>, last accessed Sept. 29, 2007).

and track[ ] pending legislation.”<sup>27</sup> In that report the author made the bold assertion that “Internet theft is not a privacy issue, but the perception that the Internet makes identity theft easier means that it is often discussed in the Internet privacy context.” This opinion was neither supported by any analysis, nor cross referenced to any other source. Identity theft is an inherent challenge to the field of internet privacy as it is only present due to the existence of privacy violations. Only through the use of fraudulent scams, the use of malware to send personal and transaction data to an outside source, hacking, and other invasions of privacy can an individual obtain the information necessary to steal a victim’s identity.

The focus on this opinion becomes important because it is an aspect of internet privacy which does not get the level of treatment it deserves in a book that claims to cover the “boiling” issues. Identity theft represents a significant threat to today’s internet user.<sup>28</sup> This threat to internet privacy cannot be justly analyzed in the mere few pages devoted to the subject. While this book can be considered a survey on issues surrounding spam and some internet privacy issues, it cannot be considered a survey on the issues of internet privacy many citizens are currently concerned about.

Kutais’s book provides those without extensive computer knowledge a framework for learning about spam and internet privacy. While this book provides policy analysis and the arguments for and against particular pieces of legislation, more focus on current internet privacy issues would have strengthened the book’s discussion.

---

<sup>27</sup> *Kutais* at 58.

<sup>28</sup> Identity theft is the largest form of fraud reported in the latest Federal Trade Commission Figures. See Federal Trade Commission: Identity Theft Victim Complaint Data, available at: [http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse\\_2006.pdf](http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf) (last accessed Feb. 7, 2007).