# บทที่ 3

# จดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์ในต่างประเทศ

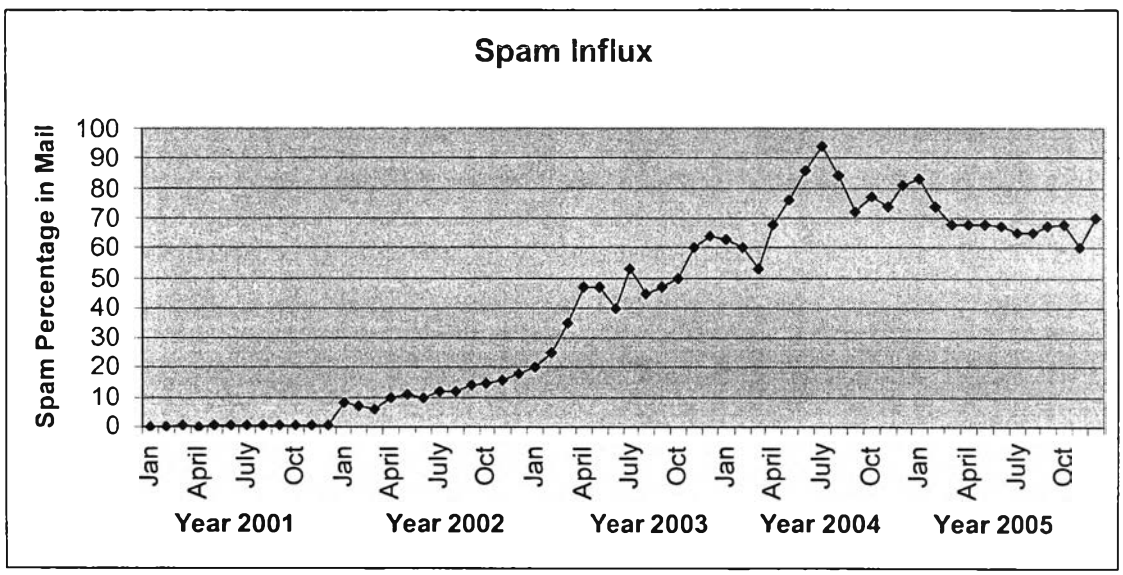
## 3.1 แนวคิดที่มีต่อปัญหาจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์ในต่างประเทศ

เมื่อโลกได้เข้าสู่ยุคของเทคโนโลยีข่าวสาร ความรวดเร็วในการสื่อสารจึงกลายมาเป็นปัจจัยสำคัญในชีวิตประจำวันของผู้คน และโลกธุรกิจอย่างมาก ยิ่งถ้าหากมีค่าใช้จ่ายที่ต่ำกว่าการสื่อสารชนิดอื่นแล้ว ก็ย่อมเป็นทางเลือกที่น่าสนใจ จดหมายอิเล็กทรอนิกส์ (E-mail) ก็เป็นอีกช่องทางหนึ่งที่ได้กลายมาเป็นช่องทางการสื่อสารที่สำคัญของโลกทุกวันนี้ และยังคงได้รับความนิยมแพร่หลายไปอีกนาน จนอาจกล่าวได้ว่าปัจจุบันนี้ ที่อยู่อีเมล (E-mail Address) ก็เป็นสิ่งจำเป็นไม่ต่างจากการมีที่อยู่ทางภูมิศาสตร์ และเนื่องจากคุณสมบัติหลายๆ อย่างของการส่งอีเมลที่เป็นข้อได้เปรียบการสื่อสารชนิดอื่นๆ ดังนั้นมันจึงกลายมาเป็นช่องทางที่สำคัญ สำหรับผู้มุ่งหวังที่จะขายสินค้า และบริการ หรือนำไปใช้ในทางที่ไม่ดี ซึ่งหลายครั้งที่เจ้าของอีเมลอาจจะได้รับอีเมลที่ตนไม่ได้รู้จักกับผู้ส่ง หรือไม่เคยมีปฏิสัมพันธ์ใดๆ กับผู้ส่งมาก่อน อีกทั้งเป็นอีเมลที่ตนไม่ต้องการ นอกจากลบทิ้งไปโดยไม่แม้แต่ที่จะเปิดอ่านอีเมลฉบับนั้น

นับตั้งแต่สแปมเมลถือกำเนิดมาในโลกของอินเตอร์เนตในช่วงราวศตวรรษที่ 19 พร้อมๆ กับความรำคาญใจของผู้คนในการจัดการกับสแปมเมล จนกระทั่งสแปมเมลได้กลายมาเป็นเครื่องมือที่สำคัญของนักการตลาดในการทำการตลาดออนไลน์ ในช่วงต้นศตวรรษที่ 20 เป็นต้นมา สแปมเมลได้ก่อให้เกิดผลกระทบต่อผู้คนในวงกว้างมากมายอย่างคาดไม่ถึง จากความรำคาญใจในการต้องใช้เวลาจัดการกับสแปมเมลที่ส่งมาในแต่ละวันในระยะแรกๆ จนกระทั่งการส่งสแปมเมลกลายเป็นสิ่งที่ได้รับความนิยมอย่างมาก และกลายเป็นวิธีการที่นักการตลาดหลายๆ คนให้ความสนใจ การหลั่งไหลเข้ามาของสแปมเมลจำนวนมากในแต่ละวัน จึงไม่เพียงแต่สร้างความรำคาญใจให้แก่ผู้รับเท่านั้น แต่ยังส่งผลกระทบหลายๆ ด้านต่อผู้ที่เกี่ยวข้องจนกลายมาเป็นปัญหาที่สำคัญของศตวรรษนี้ไปเสียแล้ว

ในประเทศที่มีความก้าวหน้าทางเทคโนโลยีสูงอย่างสหรัฐอเมริกา ประเทศในกลุ่มสหภาพยุโรป หรือญี่ปุ่น ซึ่งมีอัตราผู้ใช้อินเตอร์เนตสูงเป็นอันดับต้นๆ ของโลก ต่างก็ประสบปัญหาจาก

การส่งสแปมเมล ซึ่งกลายเป็นปัญหาสำคัญระดับชาติอย่างหลีกเลี่ยงไม่ได้ ปัญหาจากการส่งสแปมเมลในต่างประเทศนั้น ส่วนใหญ่ก็มีผลสืบเนื่องมาจากปริมาณของสแปมเมลที่มีจำนวนมากเกินไปนั่นเอง จากผลการสำรวจของ MessageLabs[1] ซึ่งเป็นบริษัทผู้ให้บริการชั้นนำของโลกด้านความปลอดภัยของข้อมูล และการจัดการด้านการบริการทางธุรกิจ และเป็นบริษัทชั้นนำในอุตสาหกรรมด้านการต่อต้านสแปมเมล ผลจากการตรวจสอบอีเมลเกือบ 10 ล้านฉบับต่อวัน ในระยะเวลาที่ผ่านมา ทั้งในนามลูกค้าของบริษัท และพันธมิตร ปรากฏแนวโน้มของอัตราการเพิ่มขึ้นของสแปมเมลที่รับส่งกันในแต่ละวัน ปรากฏตามภาพดังนี้




ภาพสถิติสแปมเมล ตั้งแต่ ปี 2001 - 2005

หากมองจากสถิติแล้วจะพบว่าแนวโน้มของจำนวนสแปมเมลที่กรองได้จากอีเมลที่รับส่งกันนั้นมีจำนวนเพิ่มมากขึ้นทุกปี ทั้งนี้ จำนวนที่เพิ่มขึ้นอย่างต่อเนื่องของสแปมเมลนี้ได้ทำให้เกิดการตื่นตัวของปัญหา ในเดือนมกราคม ปี 2003 สถิติของ MessageLabs แสดงว่าหนึ่งในอีเมล 4.1 ฉบับนั้นเป็นสแปม นั่นคือ 24.5% โดยในเดือนถัดมาอัตราส่วนเพิ่มขึ้นเป็น 1 ต่อ 3.9 หรือ 25.6% และ

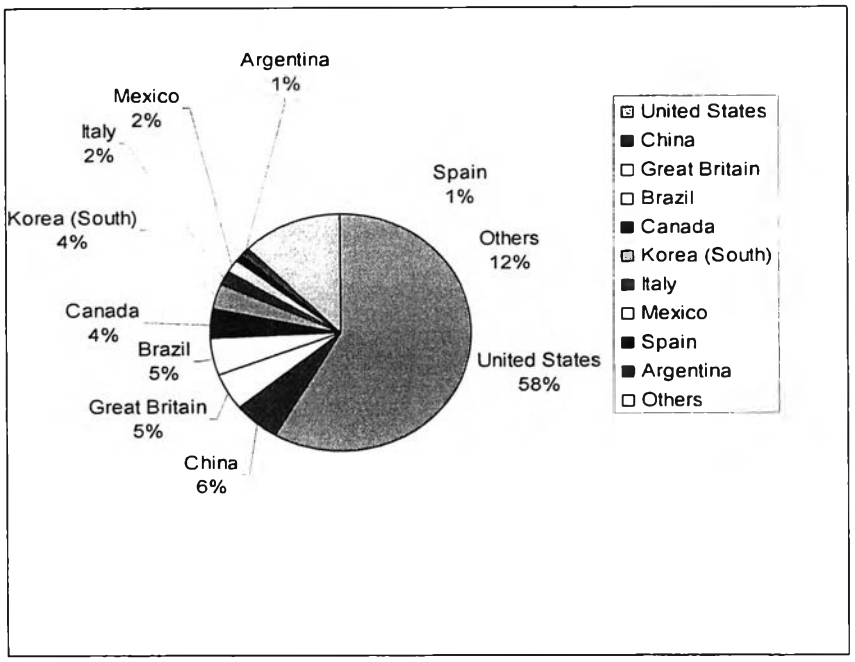
---

[1] MessageLabs. MessageLabs Intelligence Annual Email Security Report 2004[Online]. Annual Report, Dec, 2004. Available from: http://www.messagelabs.com/Threat_Watch/Intelligence_Reports/Archive (Jan, 2006)

ในเดือนมีนาคมสัดส่วนของสแปมเมลต่ออีเมลที่ถูกกฎหมายเพิ่มขึ้นเป็น 1 ต่อ 2.8 หรือ 36.3% จนกระทั่งช่วงเดือนกรกฎาคม ปี 2004 อันนับเป็นช่วงที่ตรวจพบสแปมเมลเป็นจำนวนสูงที่สุดถึง 94.5% ของอีเมลที่รับส่งทั้งหมด หรือคิดเป็นอัตราส่วนของสแปมเมลหนึ่งฉบับต่ออีเมล 1.1 ฉบับ หรืออาจกล่าวได้ว่าอีเมลที่รับส่งกันในแต่ละวันนั้น ตรวจพบว่าเป็นสแปมเมล เกือบทั้งหมด อัตราส่วนนี้เพิ่มขึ้นเป็นจำนวนมากเมื่อเทียบกับปี 2001 ที่มีจำนวนสแปมเมลเพียง 0.005% เท่านั้น

ไม่เพียงแต่ MessageLabs เท่านั้น ที่ตรวจพบสถิติการเติบโตอย่างก้าวกระโดดของสแปมเมลในช่วงระยะเวลา 2-3 ปีที่ผ่านมา (2001-2004) แต่แนวโน้มจากผลการสำรวจ และเก็บข้อมูลสแปมเมลจากเวปไซต์ และบริษัทชั้นนำหลายๆ แห่ง ที่มีการเก็บข้อมูลตลอดระยะเวลา 5 ปีที่ผ่านมา ก็มีอัตราการเติบโตที่เป็นไปในทิศทางเดียวกันทั้งหมด คือ มีอัตราการเพิ่มขึ้นอย่างต่อเนื่องตลอด และมากเกินกว่าการคาดการณ์ของสถาบันวิจัยหลายๆ แห่งในช่วงระยะเวลาเดียวกัน

ทั้งนี้ สแปมเมลที่รับส่งกันจำนวนมากบนเครือข่ายอินเตอร์เนตทุกวันนี้ มากกว่าร้อยละ 50 มีต้นกำเนิดมาจากสหรัฐอเมริกาซึ่งเป็นแหล่งกำเนิดสแปมเมลแหล่งใหญ่ที่สุดของโลก โดยมีฐานการส่งตั้งอยู่อย่างกระจัดกระจายทั่วไปในสหรัฐอเมริกา นอกจากนั้นก็จะกระจัดกระจายอยู่ตามภูมิภาคต่างๆ ทั่วไป โดยจุดมุ่งหมายของสแปมเมลเหล่านี้ ก็เพื่อเป็นการโฆษณาสินค้า และบริการ




ต้นกำเนิดสแปมเมลจากประเทศต่างๆ[2]

จากการสำรวจของผู้ให้บริการอินเตอร์เนต [3] รายใหญ่แห่งหนึ่งในสหรัฐอเมริกา รายงานว่า บริษัทได้รับสแปมเมลเกือบสองล้านฉบับในแต่ละวันจากบริษัทโฆษณา ก่อนที่จะได้รับคำสั่งให้หาทางป้องกัน ซึ่งถ้าประมาณการว่าผู้ใช้อินเตอร์เนตแต่ละรายใช้เวลาเพียง 10 วินาทีเท่านั้น ในการแยกแยะ และลบจดหมายสแปมเมล ระยะเวลาการเชื่อมต่ออินเตอร์เนตที่ถูกใช้ไปโดยผ่านผู้ให้บริการอินเตอร์เนตเพียงรายเดียวหากคิดรวมกันแล้ว อาจมากถึง 5,000 ชั่วโมงต่อวัน ยิ่งในปัจจุบันนี้ บริการการเช็คอีเมลจากเครื่องมือสื่อสารไร้สาย เช่น โทรศัพท์มือถือ หรือ อุปกรณ์ PDA ต่างๆ ไม่ใช้เรื่องยากอีกต่อไป โดยค่าใช้จ่ายในการเชื่อมต่อเครือข่ายนี้ผู้บริโภคต้องเป็นผู้รับภาระ ซึ่งถ้าหากกล่องจดหมายของตนเต็มไปด้วยสแปมเมล ผู้บริโภคก็จำต้องรับภาระในการดาวน์โหลดข้อมูลซึ่งไม่จำเป็นส่วนนี้ส่วนนี้ อันเป็นการสิ้นเปลืองค่าใช้จ่ายโดยใช่เหตุ

---

[2] Paul Wood, "A MessageLabs white paper : A spammer in the works," at http://www.messagelabs.com/Threat_Watch/White_Papers (last visited February 2006): 12.

[3] Natasha Staley, "A MessageLabs white paper : The CAN SPAM bill. A help or a hindrance?," at http://www.messagelabs.com/Threat_Watch/White_Papers (last visited February 2006): 2.

ไม่เพียงแต่ผู้ใช้อินเตอร์เนตโดยทั่วไป และผู้ให้บริการอินเตอร์เนตเท่านั้น ที่ต้องประสบปัญหาในการจัดการกับสแปมเมล ในส่วนของภาคธุรกิจต่างๆ ที่มีระบบเมลเซิร์ฟเวอร์เป็นของตนเอง โดยมีวัตถุประสงค์เพื่อความสะดวกในการติดต่อกันระหว่างบุคลากรในองค์กรของตน และบุคคลภายนอก ต่างก็ต้องประสบปัญหาจากการโจมตีของสแปมเมลทั้งนั้น การหลั่งไหลเข้ามาจำนวนมากของสแปมเมล นอกจากจะทำให้สูญเสียเวลาการทำงานต่อวันของลูกจ้างในการจัดการกับสแปมเมลแล้ว หากสแปมเมลมีจำนวนมากเกินไปจนทำให้การสื่อสารในองค์กรเกิดการชะงัก หรือระบบเกิดความเสียหายเพราะสแปมเมลมีไวรัสติดมาด้วย ความสูญเสียที่เกิดขึ้นก็จะเป็นความสูญเสียที่มากขึ้นเป็นทวีคูณ

จากรายงานการวิจัยของ Ferris Research [4] ซึ่งเป็นบริษัทวิจัยชั้นนำทางด้านเทคโนโลยีในสหรัฐอเมริกา ได้ประมาณการว่าในช่วงปี 2003 สแปมเมลเหล่านี้ก่อให้เกิดต้นทุนต่อภาคธุรกิจในสหรัฐอเมริการวมกันมากกว่า 10 พันล้านเหรียญดอลล่าห์สหรัฐ หรือคิดเฉลี่ยเป็น 14 เหรียญดอลล่าห์สหรัฐ ต่อผู้ใช้หนึ่งคน ซึ่งเพิ่มขึ้นจาก 8.9 พันล้านเหรียญดอลล่าห์สหรัฐ จากการประมาณการในระหว่างปี 2002 ประมาณการความเสียหายดังกล่าวนี้ ทำให้หลายๆ บริษัทหันมาให้ความสนใจในการปกป้องข้อมูล และระบบคอมพิวเตอร์ภายในองค์กรของตนมากยิ่งขึ้น โดยการใช้บริการโปรแกรมต่อต้านสแปมเมลต่างๆ ซึ่งเป็นมาตรการทางเทคโนโลยีที่มีค่าใช้จ่ายสูง ค่าใช้จ่ายต่างๆ ที่เกิดขึ้นนี้ ในท้ายที่สุดแล้ว ก็ตกอยู่กับผู้บริโภคโดยทั่วไปนั่นเอง

ยิ่งไปกว่านั้นในต่างประเทศ สแปมเมลยังก่อให้เกิดความเสี่ยงทางกฎหมายในการฟ้องคดีของลูกจ้างต่อภาคธุรกิจ[5] จากการถูกคุกคามจากสแปมเมลภาพลามกต่างๆ จากภายนอก หรือจากการส่งต่อสแปมเมลจากผู้ร่วมงานภายในองค์กรเอง ซึ่งอาจก่อให้เกิดคดีความขึ้นได้ เพราะผู้ประกอบการมีหน้าที่ที่จะต้องปกป้องลูกจ้างของตนจากสื่อดิจิตอลที่ผิดกฎหมาย และเนื้อหาของอีเมลที่ไม่เหมาะสมภายในองค์กรของตน ความเสี่ยงต่อคดีความทางกฎหมายอาจส่งผลผลให้เกิดการจัดตั้งค่าชดเชยซึ่งเป็นต้นทุนที่เพิ่มขึ้นในทางธุรกิจ และยังทำให้ความน่าเชื่อถือของบริษัทหมดไปหากถูกดำเนินคดี เนื่องจากมาตรการที่เหมาะสมในการต่อสู้กับสแปมเมลไม่มีประสิทธิภาพเพียงพอ

---

[4] เรื่องเดียวกัน.

[5] Paul wood, "MessageLabs white paper, A spammer in the works: Everything you need to know," at http://www.messagelabs.com/Threat_Watch/White_Papers (last visited February 2006): 5.

ความเสียหายจากการถูกปลอมแปลงโดเมนเนม เพื่อนำมาใช้ในการส่งสแปมเมล หรือการแอบอ้างใช้ความมีชื่อเสียง และความเป็นที่รู้จักของบริษัทใหญ่หลายๆ แห่ง เพื่อนำไปใช้ในการปลอมแปลงเนื้อหา เพื่อดึงดูดความสนใจของผู้รับในการเปิดอ่านสแปมเมลเหล่านั้น ก็เป็นอีกปัญหาหนึ่งที่หลายฝ่ายให้ความสนใจ ซึ่งบริษัทใหญ่หลายแห่งในสหรัฐอเมริกาต่างก็ประสบปัญหานี้มาแล้ว เช่น Ebay, Citybank, AOL, Microsoft หรือแม้แต่สถาบันการศึกษาที่มีชื่อเสียงหลายๆ แห่งในอเมริกาก็ล้วนแล้วแต่ถูกแอบอ้างชื่อเพื่อใช้ดึงดูดความสนใจของผู้รับในการเปิดอ่านสแปมเมลทั้งนั้น เหล่านี้ไม่เพียงแต่ส่งผลกระทบถึงความมีชื่อเสียง และความน่าเชื่อถือขององค์กรเท่านั้น แต่ยังส่งผลกระทบต่อธุรกิจที่ทำอย่างหลีกเลี่ยงไม่ได้ หลายครั้งที่ ISP และเจ้าของโดเมนเนมที่ถูกลักลอบใช้โดยไม่ได้รับอนุญาต ต้องถูกขึ้นบัญชีดำจากองค์กรต่างๆ ในฐานะที่เป็นผู้กระจายสแปมเมล ซึ่งทำให้อีเมลใดๆ ก็ตามที่ถูกส่งมาจากโดเมนเนมนี้ ไม่สามารถส่งไปยังปลายทางที่มีการบล็อกโดเมนเนม หรือใช้โปรแกรมต่อต้านสแปมเมลโดยอาศัยจากรายชื่อโดเมนเนมที่ถูกขึ้นบัญชีไว้กับองค์กรต่างๆ นี้ได้ ความเสียหายที่เกิดขึ้นนี้ ISP และเจ้าของโดเมนเนมที่ถูกลักลอบนำไปใช้โดยไม่ได้รับอนุญาต ต้องอาศัยความพยายามอย่างมากเพื่อให้พ้นจากการถูกขึ้นบัญชี และกลับมาออนไลน์ได้ใหม่อีกครั้ง หลังจากถูกโจมตีด้วยสแปมจำนวนมหาศาล และอีเมล ของผู้ที่ไม่พอใจจำนวนมาก เป็นสาเหตุให้พวกเขาต้องประสบกับปัญหาทางเศรษฐกิจอย่างหนักจากการสูญเสียโอกาสทางธุรกิจ และเวลาที่เสียไปในการพยายามกลับมาออนไลน์ใหม่อีกครั้ง ซึ่งก่อให้เกิดความเสียหายอย่างมากต่อสมาชิกของโดเมนเนมนั้นๆ หากเกิดขึ้นบ่อยครั้งก็อาจเป็นเหตุให้มีการบอกเลิกการเป็นสมาชิก และเปลี่ยนไปใช้บริการจากผู้ให้บริการอินเตอร์เนตรายอื่น ซึ่งเป็นธุรกิจที่มีอัตราการแข่งขันกันสูง

ผลกระทบต่างๆ ที่กล่าวมาทั้งหมดนี้ ทำให้สแปมเมลกลายเป็นปัญหาในลำดับต้นๆ ที่หลายๆ ประเทศให้ความสนใจ และพยายามหาทางแก้ไข จากผลการสำรวจธุรกิจ 50 แห่งที่ประสบปัญหาจากการโจมตีของสแปมเมลโดย Radicati Group[6] ในเดือนมิถุนายน 2003 พบว่า ร้อยละ 52 กล่าวว่าการลดจำนวนสแปมคือภาระกิจที่ต้องทำเป็นอันดับแรกในอีก 18 เดือนข้างหน้า นอกจากนั้นผลการสำรวจฝ่ายบริหารเทคโนโลยี 400 แห่ง ร้อยละ 70 ให้ข้อมูลว่า การลดจำนวนสแปมลงเพื่อปกป้องผลประโยชน์ของธุรกิจเป็นภารกิจหลักขององค์กรในระหว่างปี 2004 ในขณะที่ร้อยละ 65 วางแผนที่จะลงทุนในโปรแกรมต่อต้านสแปม และกลั่นกรองอีเมล ซึ่งเพิ่มขึ้นจากร้อยละ 51 ในปี 2003

---

[6] Natasha Staley, "A MessageLabs white paper : The CAN SPAM bill. A help or a hindrance?," at http://www.messagelabs.com/Threat_Watch/White_Papers (last visited February 2006): 2.

ด้วยต้นทุนที่ต่ำในการทำการตลาดออนไลน์โดยการส่งสแปมเมล ทำให้คาดการณ์ได้ว่าสแปมเมลจะยังคงอยู่คู่กับอินเตอร์เนตต่อไปอีกนานเท่านาน ตราบใดที่ยังไม่มีช่องทางการสื่อสารแบบใหม่ ที่มีประสิทธิภาพ และมีค่าใช้จ่ายน้อยกว่าการส่งสแปมเมลเกิดขึ้น อีกทั้งผลตอบแทนที่คุ้มค่าจากการทำธุรกิจนี้ จึงดึงดูดสแปมเมอร์หน้าใหม่ให้เข้ามาร่วมทำธุรกิจไม่น้อย ดังนั้น หลายๆ ประเทศทั่วโลกจึงได้เล็งเห็นความสำคัญของปัญหานี้ เนื่องจากผลกระทบที่เกิดขึ้น อาจก่อให้เกิดความสูญเสียต่อทรัพยากรของประเทศอย่างมาก ซึ่งหากปล่อยเอาไว้นอกจากจะทำให้ปัญหาทวีความรุนแรงขึ้นแล้ว ยังเป็นการเปิดช่องทางให้สแปมเมอร์หลีกเลี่ยงกฎหมายจากประเทศที่มีบทบัญญัติโดยชัดเจนในเรื่องนี้เข้ามาอาศัยช่องว่างทางกฎหมายในประเทศตนเป็นแหล่งในการแพร่กระจายสแปมเมลแหล่งใหม่อีกด้วย หลายประเทศจึงมีความพยายามอย่างมากที่จะหาวิธีในการแก้ไขปัญหา ทั้งทางด้านเทคโนโลยีและการใช้มาตรการทางกฎหมาย โดยพยายามศึกษา และค้นหาแนวทางที่เหมาะสมในการแก้ปัญหากับประเทศของตน ก่อนที่ปัญหาจะลุกลามไปจนยากที่จะควบคุม ซึ่งอย่างน้อยก็นับว่าเป็นการเริ่มต้นที่ดีในการจัดการกับปัญหาที่มาพร้อมกับเทคโนโลยีที่ทันสมัย และก้าวไปข้างหน้าอย่างรวดเร็ว ก่อนที่จะสายเกินแก้

**3.2 ความพยายามเบื้องต้นกับมาตรการในการแก้ไขปัญหาสแปมเมลในต่างประเทศ**

ในขณะที่ ปัญหาเรื่องสแปมเมลได้กลายเป็นปัญหาใหญ่กับผู้ใช้อินเตอร์เนตทั่วโลกด้วยเหตุนี้ ในหลายประเทศที่มีการใช้เทคโนโลยีสารสนเทศอย่างแพร่หลาย จึงได้มีความพยายามที่จะหามาตรการในการแก้ไขปัญหาเรื่องสแปมเมลโดยวิธีต่างๆ เท่าที่จะสามารถกระทำได้ในขณะนั้น ซึ่งสามารถแบ่งออกเป็น 3 ประเภท[7]

3.2.1 ความพยายามเบื้องต้น (Informal Approaches)

เป็นการสร้างมารยาททางสังคมของการใช้อินเตอร์เนต รวมทั้งการทำข้อตกลงและการออกกฎเกณฑ์ หรือหลักจริยธรรมระหว่างกันในอุตสาหกรรมอินเตอร์เนตเพื่อควบคุมกันเอง เช่น การออกนโยบายห้ามการส่งสแปมเมลตามเวปไซท์ที่ให้บริการฟรีอีเมลหลายแห่งใน Terms & Conditions เช่น Hotmail, Yahoo, Google หรือการห้ามส่งสแปมเมลโดยผ่าน ISP ตาม นโยบาย

---

[7] อรรยา สิงห์สงบ, "ความพยายามทางกฎหมายกับการแก้ไขปัญหาจดหมายอิเลคทรอนิกส์ขยะ (Spam Mail)," นักบริหาร 23,4 (ต.ค. – ธ.ค. 2546) : 84-90.

ทั้งหลายที่ได้ประกาศไว้อย่างชัดเจน อย่างไรก็ตามนโยบายดังกล่าวแทบไม่ส่งผลอะไรกับผู้ส่งสแปมเมลเลย เนื่องจากข้อตกลง หรือนโยบายที่ออกมานั้นขาดประสิทธิภาพในการใช้บังคับได้จริงกับผู้ฝ่าฝืน

นอกจากนี้การให้ความรู้แก่ประชาชนชาวเนต (Netizen) ถึงข้อควรระวังเบื้องต้นจากการใช้อินเตอร์เนตก็เป็นสิ่งสำคัญที่หลายฝ่ายให้ความสนใจ เนื่องจากหากผู้ใช้อินเตอร์เนตโดยทั่วไปมีความระมัดระวังตัว ไม่พยายามทิ้งร่อยรอยของตน หรืออีเมลเอาไว้หลังจากการเข้าไปใช้เวปไซท์ หรือข้อมูลข่าวสารต่างๆ ก็จะเป็นการป้องกันตัวเองในระดับหนึ่งจากการถูกสแปม โดยการหลีกเลี่ยงการระบุที่อยู่อีเมลของตนเอาไว้ในสถานที่สาธารณะบนอินเตอร์เนต ซึ่งถ้าหากมีความจำเป็นก็ควรจะมีเทคนิคเช่น การใช้คำว่า at แทนเครื่องหมาย @ ในการระบุอีเมลของตน หรือการใช้วิธีการเขียนอธิบายชื่อที่อยู่อีเมลของตนเพื่อให้ผู้อ่านโดยทั่วไปสามารถเข้าใจได้ ทั้งนี้ เพื่อหลีกเลี่ยงการใช้โปรแกรมค้นหาและรวบรวมอีเมลของสแปมเมอร์ การไม่ซื้อสินค้า การไม่ตอบกลับอีเมล ที่ส่งมาพร้อมกับสแปมเมลต่างๆ ก็เป็นอีกวิธีหนึ่งที่จะช่วยลดสแปมเมลลงได้

แม้ว่าความพยายามต่างๆ เหล่านี้ จะไม่ประสบผลสำเร็จมากนัก และถึงแม้จะระมัดระวังตัวมากแค่ไหนก็ตาม ก็อาจจะไม่สามารถหลีกเลี่ยงการตกอยู่ในบัญชีส่งเมลของสแปมเมอร์ได้เต็มร้อยเปอร์เซ็นต์ แต่ก็ถือว่าเป็นมาตรการป้องกันตนเอง ไม่ให้ตกอยู่ในบัญชีการส่งเมลของสแปมเมอร์ได้ในช่วงระยะเวลาหนึ่ง

3.2.2 ความพยายามทางเทคนิค (Technical Approaches)

มาตรการทางเทคนิคในการป้องกันสแปมเมล เป็นวิธีการที่มีประสิทธิภาพมากขึ้นในระดับหนึ่งที่ผู้ให้บริการอินเตอร์เนต ผู้บริโภค และภาคธุรกิจหลายๆ แห่งเลือกใช้ ซึ่งก็มีทั้งที่สามารถดาวน์โหลดมาใช้ได้ฟรี และที่ต้องเสียค่าใช้จ่าย ซึ่งเป็นโปรแกรมที่พัฒนาขึ้นมาเพื่อให้ผู้ใช้อินเตอร์เนตเอง ผู้ให้บริการอินเตอร์เนต หรือผู้ควบคุมปลายทาง กลั่นกรอง และป้องกันสแปมเมลที่จะถูกส่งเข้ามาในกล่องจดหมาย หรือเซิร์ฟเวอร์ของตน (Filtering and Blocking) ซึ่งโปรแกรมเหล่านี้ก็มีอยู่มากมาย เช่น โปรแกรมของ Brightmail, Spambam, Spamtrap, Spamcop, Spamkiller, Surfcontrol เป็นต้น ซึ่งค่าใช้จ่ายในซื้อโปรแกรมต่างๆ รวมถึงค่าใช้จ่ายในการติดตั้ง และบำรุงรักษามาตรการทางเทคนิคเพื่อป้องกันระบบอีเมล และเซิร์ฟเวอร์ของตน ก็เป็นค่าใช้จ่ายที่สูงทีเดียว แต่ก็นับว่าคุ้มค่าหากเทียบกับค่าใช้จ่ายที่ต้องสูญเสียไปจากการโจมตีจากสแปมเมล

วิธีการทำงานของโปรแกรมต่างๆ [8] เหล่านี้ก็มีด้วยกันหลายวิธี ซึ่งก็มีตั้งแต่วิธีการวิเคราะห์เนื้อหาของอีเมล ว่าเข้าข่ายจะเป็นสแปมเมลหรือไม่ โดยดูจากถ้อยคำที่เป็นที่นิยมใช้ในการส่งสแปมเมล เช่น XXX, Get Rich Quick, Loan, Urgent รวมถึงการบล๊อกโดเมนเนมที่ถูกขึ้นบัญชีไว้ว่ามีประวัติในการกระจายสแปมเมล โดยดูจาก IP Address ที่เรียกว่า Blacklisting หรือการสันนิษฐานว่าอีเมลทุกฉบับสามารถส่งเข้ามาได้ แต่ต้องมีการยืนยันตัวตนของผู้ส่งเสียก่อน หรือ Whitelisting เป็นต้น ซึ่งรูปแบบที่โปรแกรมต่างๆ ใช้ยังมีอีกมากมายหลายวิธี เพื่อให้การกลั่นกรองสแปมเมลมีประสิทธิภาพมากขึ้น รวมถึงการพัฒนาโปรแกรมใหม่ๆ เพื่อให้สามารถก้าวล้ำกับการพัฒนาใหม่ๆ ของสแปมเมลได้

อย่างไรก็ตาม การใช้โปรแกรมเพื่อกรองสแปมเมลที่มีประสิทธิภาพสูง ก็ย่อมมีความเสี่ยงต่อการกรองอีเมลที่ถูกกฎหมายด้วยความเข้าใจว่าเป็นสแปมเมลออกไปด้วย ทั้งนี้ อัตราส่วนของความมีประสิทธิภาพของโปรแกรม มีความสัมพันธ์กับอัตราส่วนของความผิดพลาดที่อาจเกิดขึ้นได้ ซึ่งหากเกิดขึ้นแม้เพียง 0.1% ในภาพธุรกิจ ก็อาจจะนำความเสียหายมหาศาลมาสู่ธุรกิจที่ดำเนินการได้

3.3.3 ความพยายามทางกฎหมาย (Legal Approaches)

มาตรการดังกล่าวข้างต้นนั้น แม้จะมีประสิทธิภาพในการป้องกันสแปมเมลได้ในระดับหนึ่ง แต่ก็มิได้ทำให้ปริมาณการเพิ่มขึ้นของสแปมเมลลดลงแต่อย่างใด ทั้งนี้เห็นได้จากการเพิ่มขึ้นอย่างต่อเนื่องของจำนวนสแปมเมลในแต่ละปี และความรุนแรงของปัญหาที่ทวีมากขึ้นทุกปี เพราะเมื่อมีมาตรการ หรือเทคโนโลยีในการกลั่นกรองสแปมเมลใหม่ๆ ออกมา สแปมเมอร์ก็จะหาวิธีการใหม่ๆ เช่นกัน ในการหลีกเลี่ยงจากการดักจับ หรือกลั่นกรองจากเครื่องมือเหล่านั้น ทำให้ไม่สามารถควบคุมสแปมเมลได้อย่างจริงจัง หลายครั้งที่ผู้ให้บริการอินเตอร์เนต และภาคธุรกิจหลายๆ แห่งต้องประสบปัญหาจากการถูกโจมตีของสแปมเมลจำนวนมากเข้ามาในระบบ ทำให้ระบบเกิดความขัดข้อง และเป็นการสิ้นเปลืองทรัพยากรของบริษัทโดยใช่เหตุ หลายๆ บริษัท จึงพยายามที่จะหาทางป้องกันทรัพยากรของตนให้ปลอดภัยจากการถูกโจมตี ควบคู่กันไปกับมาตรการต่างๆ ข้างต้น ซึ่งหลายๆ ครั้งความพยายามดังกล่าวก็ไม่ประสบผลสำเร็จเท่าใดนัก ดังนั้น วิธีที่จะจัดการกับสแปมเมอร์เหล่านี้ให้ได้ผลในท้ายที่สุดแล้ว จึงจำเป็นต้องอาศัยมาตรการทางกฎหมายที่มีอยู่ประกอบเข้าไปด้วย เพื่อใช้เป็นเครื่องมือที่สำคัญในการจัดการกับต้นเหตุของปัญหา

---

[8] Paul wood, "MessageLabs white paper, A spammer in the works: Everything you need to know," at http://www.messagelabs.com/Threat_Watch/White_Papers (last visited February 2006): 14.

อย่างไรก็ดี ด้วยเหตุที่สแปมเมลมีลักษณะเฉพาะอันเกิดจากการสื่อสารทางอินเตอร์เนต รวมถึงมีรูปแบบ และวิธีการแบบใหม่ๆ ที่เพิ่งได้รับความนิยมในไม่กี่ปีที่ผ่านมานี้ ดังนั้นการปรับใช้กฎหมายที่มีอยู่แล้ว เพื่อจัดการกับสแปมเมล จึงไม่อาจรับรองได้ว่า จะประสบผลสำเร็จไปทั้งหมด โดยเฉพาะในสหรัฐอเมริกา ซึ่งมากกว่า 50% ของสแปมเมลทั้งหมดมีต้นกำเนิดจากที่นี่ ในช่วง 4-5 ปีที่ผ่านมา ที่หลายบริษัทต้องประสบปัญหาอย่างหนักจากการถูกลักลอบใช้ทรัพยากรทางเทคโนโลยีข้อมูลการสื่อสารของตน เป็นที่ส่งสแปมเมล ในขณะที่ยังไม่มีกฎหมายโดยเฉพาะของรัฐบาลกลางออกมาใช้เพื่อควบคุมสแปมเมล บริษัทต่างๆ จึงต้องหาทางเอาผิดกับสแปมเมอร์ ต่อมูลค่าความเสียหายที่เกิดขึ้นแก่บริษัทของตน ทั้งนี้ก็โดยการนำกฎหมายที่มีอยู่มาปรับใช้ให้สอดคล้องกับสถานการณ์จริงที่เกิดขึ้น ซึ่งจะได้ผล หรือศาลจะรับฟ้องหรือไม่ อย่างไร ก็ขึ้นอยู่กับมูลเหตุของคดี และการพิสูจน์ความเสียหายของโจทก์เอง และยังรวมถึงการดีความกฎหมาย และการปรับใช้กฎหมายของผู้พิพากษาในแต่ละคดีว่าจะมีความเห็น และตีความในเรื่องนั้นๆ อย่างไร ซึ่งแน่นอนว่าแม้จะมีเหตุของคดีที่คล้ายกันก็ตาม แต่ผลของคดีก็อาจมีความแตกต่างกันไปก็ได้ ตามปัจจัยดังที่กล่าวมาแล้วเป็นสำคัญ นอกจากนี้ ในประเทศที่มีการปกครองแบบสหพันธรัฐ อย่างสหรัฐอเมริกา แต่ละรัฐก็จะมีการบัญญัติกฎหมายต่อด้านสแปมเมลซึ่งก็มีเนื้อหา และมาตรการที่แตกต่างกันออกไป ทำให้เกิดปัญหาในเรื่องการบังคับใช้กฎหมาย และสร้างความสับสนต่อประชาชนผู้ที่ต้องปฏิบัติตามกฎหมายเป็นอย่างยิ่ง ในขณะที่สแปมเมลเป็นปัญหาที่ไม่อาจจำกัดขอบเขตทางภูมิศาสตร์ได้

อย่างไรก็ตาม ความพยายามทางกฎหมายกับการจัดการกับสแปมเมลก็นับว่าเป็นสิ่งจำเป็น อันเป็นการแสดงถึงขีดความอดทนของหลายฝ่ายต่อปัญหาเรื่องสแปมเมลในขณะที่ยังไม่มีกฎหมายโดยเฉพาะออกมาจัดการ และควบคุมกับปัญหานี้

**3.3 เหตุใดจึงต้องมีกฎหมายเฉพาะเพื่อใช้จัดการกับสแปมเมล**

อย่างที่ได้กล่าวไปในหัวข้อก่อนแล้ว ถึงความรุนแรงของปัญหาในต่างประเทศ และมาตรการต่างๆ ที่หลายประเทศนำมาใช้ อย่างไรก็ดี มาตรการเหล่านั้น ก็ไม่สามารถยืนยันถึงความปลอดภัยที่จะไม่ถูกโจมดีจากสแปมเมลได้ ทั้งนี้ แต่ละมาตรการต่างก็มีทั้งข้อดี และข้อด้อยในตัวเอง กล่าวคือ

1. การขาดประสิทธิภาพในการใช้บังคับได้จริงระหว่างกัน ไม่ว่าจะเป็นการกำหนดข้อตกลงและเงื่อนไขต่างๆ ในการสมัครเป็นสมาชิกฟรีอีเมลต่างๆ ซึ่งหากผิดข้อตกลง ก็เพียงแต่ระงับที่อยู่อีเมลเดิมเพื่อเปลี่ยนไปใช้ที่อยู่ใหม่ หรือเปลี่ยนไปใช้บริการอินเตอร์เนตรายอื่น ซึ่งนับว่าเป็นเรื่องง่ายสำหรับสแปมเมอร์ ทั้งนี้ยังไม่นับรวมการลักลอบใช้เซิร์ฟเวอร์ของผู้อื่นในการเป็นแหล่ง

กระจายอีเมล นอกจากนั้นวิธีการในการกรองสแปมเมล เช่น การบล็อกโดเมนเนม หรือการบล็อกจากผู้ให้บริการอินเตอร์เนต ยังเป็นการสนับสนุนให้มีการปลอมแปลงเพิ่มมากยิ่งขึ้น เพื่อหลีกเลี่ยงจากดักจับจากโปรแกรมต่างๆ อันทำให้เป็นการเพิ่มจำนวนสแปมเมลให้มากขึ้นไปอีก

2. ค่าใช้จ่ายที่สูงในการติดตั้งโปรแกรมต่อต้านสแปม ทั้งนี้ หากต้องการโปรแกรมต่อต้านสแปมเมลที่มีประสิทธิภาพก็ย่อมต้องแลกกับค่าใช้จ่ายที่สูงตามส่วนไปด้วย ซึ่งก็อาจจะไม่เหมาะกับผู้ใช้โดยทั่วไป ในการต้องเสียเงินเพิ่มขึ้นเพื่อป้องกันตนเองจากสแปมเมล อีกทั้งประสิทธิภาพในการกรองสแปมเมลที่สูง ย่อมต้องแลกกับความเป็นส่วนตัวที่ต้องสูญเสียไป และโอกาสผิดพลาดที่อีเมลส่วนตัว จะถูกจัดว่าเป็นสแปมเมลได้ง่ายเช่นกัน

3. ความไม่แน่นอนในการบังคับใช้กฎหมายอื่นๆ ในการจัดการกับ สแปมเมล ในฐานะบทกฎหมายที่ใกล้เคียง แม้ว่าผู้คนจะมีความโกรธแค้นจนต้องหามาตรการทางกฎหมายมาจัดการกับสแปมเมอร์มากมายเพียงใด แต่การปรับใช้บทกฎหมายที่ใกล้เคียงอย่างยิ่ง ก็ไม่อาจเป็นเครื่องรับประกันได้ว่าศาลจะเห็นพ้องด้วยในมูลคดี อีกทั้งการพิสูจน์ถึงความเสียหายจากการถูกโจมตีจากสแปมเมล ก็เป็นภาระที่หนักหนาพอควร สำหรับโจทก์

ดังนั้น หลังจากที่ได้พยายามทุกวิถีทางแล้ว ก็ยังไม่ประสบผลสำเร็จเท่าที่ควร ทางออกในการมีกฎหมายเฉพาะเกี่ยวกับเรื่องนี้จึงเป็นมาตรการสุดท้ายในการจัดการกับสแปมเมล ซึ่งมีลักษณะไม่สามารถระบุแหล่งที่มาได้โดยชัดเจน และอาจประสบปัญหาในเรื่องข้อจำกัดของเขตอำนาจ

อย่างไรก็ดี การส่งสแปมเมล ก็ไม่ใช่เรื่องที่ยอมรับกันไม่ได้เสียทีเดียว ทั้งนี้ เห็นได้จากวิธีการทำการตลาดโดยตรงซึ่งเป็นสิ่งที่เกิดขึ้นมานานแล้ว โดยอาจมีรูปแบบที่แตกต่างกันออกไป เช่น การขายสินค้าโดยการเดินขายของตามบ้าน การทำโบรชัวร์โฆษณา การส่งแฟกซ์ การใช้โทรศัพท์ จนมาถึงการส่งสแปมเมล การที่บริษัทหนึ่งทำการตลาดโดยวิธีการส่งสแปมเมลออกไปอย่างถูกกฎหมาย กล่าวคือ ส่งไปยังผู้ที่สมัครรับข่าวสารของตน และมีวิธีการให้ยกเลิกการรับอีเมลดังกล่าวได้ในอนาคตอีกด้วย ดังนี้ กฎหมายก็ไม่ควรเข้าไปแทรกแซง หรือทำให้เกิดข้อยุ่งยากในการทำธุรกิจของบริษัทที่ปฏิบัติอย่างเคร่งครัดต่อความสมัครใจของลูกค้าอยู่แล้ว แต่เหตุผลที่ต้องมีมาตรการทางกฎหมายเฉพาะกับการจัดการกับปัญหานี้ ก็คือ

1. เพื่อควบคุมการเพิ่มจำนวนขึ้นอย่างรวดเร็วและต่อเนื่องของสแปมเมล การเพิ่มขึ้นอย่างควบคุมไม่ได้ดังว่านี้จะปรากฏขึ้นอย่างแน่นอน เพราะว่าความดึงดูดทางเศรษฐกิจ สแปมเมล จึงได้รับความนิยมด้วยเหตุผล 2 ประการ คือ สามารถเข้าถึงกลุ่มคนจำนวนมาก ด้วยต้นทุนเพียง

น้อยนิดเมื่อเทียบกับวิธีการทำการตลาดโดยทั่วไป และกลุ่มผู้บริโภคเหล่านี้มักเป็นกลุ่มผู้บริโภคที่มีการศึกษาดี ดังนั้นจึงมีฐานะทางการเงินที่มั่นคงด้วย

2. เพื่อควบคุมความเหมาะสมด้านเนื้อหากับผู้รับ เนื้อหาของสแปมเมลส่วนใหญ่กว่าร้อยละ 90% มักจะเป็นเรื่องเกี่ยวกับการโฆษณาสินค้า และบริการ แต่ก็ยังมีสแปมเมลในรูปแบบอื่นๆ อีกมากมาย เช่น การเมือง ศาสนา หรือสแปมเมลที่มีเนื้อหาหลอกลวง หลอกให้เชื่อต่างๆ ซึ่งบางครั้งเนื้อหาของสแปมเมลก็ไม่เหมาะสมกับวัยของผู้รับ ในต่างประเทศแม้ว่าจะยอมรับถึงสิทธิและเสรีภาพในการแสดงความคิดเห็นอย่างมาก แต่กฎหมายก็มิได้ละเลยคำนึงถึงความเหมาะสมของผู้รับกับเนื้อหาดังกล่าว ทั้งนี้ ผู้เยาว์ก็ไม่ควรถูกยัดเยียดด้วยสแปมเมลที่มีเนื้อหาเป็นการโฆษณาสินค้าสำหรับผู้ใหญ่ หรือการบริการทางเพศต่างๆ ที่สำคัญการปล่อยให้มีสแปมเมลดังกล่าวแพร่หลายอยู่บนอินเตอร์เนตโดยไร้ซึ่งมาตรการควบคุมใดๆ แล้ว ย่อมส่งผลเสียต่อคนในสังคมนั้นอย่างหลีกเลี่ยงไม่ได้

3. เพื่อหยุดยั้งการกระทำที่ผิดกฎหมายโดยอาศัยสแปมเมล วิธีการที่สแปมเมอร์ใช้นั้น มักแสดงถึงความไม่จริงใจ และซื่อสัตย์ต่อผู้บริโภค ซึ่งหากปล่อยให้มีการทำการตลาด หรือการส่งสแปมเมลออกไปโดยผู้ส่งไม่ได้มีความจริงใจในการเปิดเผยแหล่งที่มา เช่น ที่อยู่อีเมลที่แท้จริงหรือที่สามารถติดต่อกลับไปได้ รวมถึงการไม่ซื่อสัตย์ต่อการบอกเลิกการรับอีเมลจากผู้รับแล้ว ปัญหาก็จะลุกลามใหญ่โตดังที่เป็นเช่นทุกวันนี้ สแปมเมอร์ส่วนใหญ่มักใช้วิธีการที่เรียกว่า E-mail Spoofing[9] ในการปลอมแปลงชื่อผู้ส่ง โดยปกติเมื่อเราได้รับอีเมลจากใครสักคน สิ่งที่ใช้สำหรับยืนยันตัวตนคน ๆ นั้น คือ อีเมลแอดเดรส ที่ปรากฏอยู่ในส่วนของผู้ส่งอีเมลฉบับนั้น ทำให้เราสามารถทราบได้ในทันทีว่าใครเป็นผู้ส่ง แต่เราอาจจะได้รับอีเมลจากใครคนหนึ่งซึ่งใช้ชื่ออีเมล แอดเดรสปลอมที่ปรากฏอยู่ในอีเมลก็ได้ วิธีการปลอมแปลงอีเมลที่สแปมเมอร์นิยมใช้ คือ การ telnet ไปที่ Port หมายเลข 25 เป็นการติดต่อโดยตรงกับ Port ของ SMTP (Simple Mail Transport Protocol) ซึ่งเป็นโปรโตคอลสำหรับการส่งเมล เมื่อเชื่อมต่อได้แล้ว ก็เพียงพิมพ์คำสั่งต่อไปนี้

> telnet < SMTP hostname > 25

> HELO < spoofed domain >

> MAIL FROM: < spoofed sender's email address >

> RCPT TO: < recipient's email address>

---

[9] No.18, "ปฏิบัติการป้องกันการดูโจม Mailbox," ที่ http://www.designpartv.com/tutorials/view.php?cid=00437(26 พฤษภาคม 2546).

> DATA < press enter >

< message > < press enter >

< finish with > < press enter >

> QUIT

ข้อความที่ระบุหลังจากการพิมพ์คำว่า DATA จะเป็นส่วนที่สแปมเมอร์สามารถระบุข้อความปลอมอะไรก็ได้ที่ต้องการ โดยอาจจะเปลี่ยนชื่อผู้ส่ง ชื่อผู้รับเป็นคนอื่นก็ได้ เพราะจะเป็นส่วนที่ปรากฏในอีเมลที่ผู้รับได้รับ แต่เมลเซิร์ฟเวอร์บางตัว ผู้ดูแลก็ได้ทำการตั้งค่าไว้เพื่อเป็นการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาต อาศัยเซิร์ฟเวอร์ของตนในการส่งเมลออกไป ซึ่งเรียกว่าการทำ Mail Relay โดยการระบุหมายเลข IP หรือชื่อโดเมนที่อนุญาตให้ใช้เท่านั้นไว้ในโปรแกรมส่งเมล

นอกจากนั้น สแปมเมลที่มีเนื้อหาหลอกลวง ก็ได้รับความนิยมอย่างมาก ซึ่งรูปแบบก็มีทั้ง การสร้างเรื่องหลอกลวงต่างๆ เพื่อหวังประโยชน์จากความโลภของผู้รับ หรือการสร้างเวปไซท์ขึ้นมาเพื่อเลียนแบบเวปไซท์ที่มีชื่อเสียง โดยเฉพาะด้านการเงิน การธนาคาร เพื่อหลอกลวงให้ผู้รับคลิ๊กเข้าไปในเวปไซท์เพื่อยืนยันข้อมูลส่วนบุคคล เช่นข้อมูลบัตรเครดิต ข้อมูลบัญชีธนาคารต่างๆ หากใครหลงเชื่อใส่ข้อมูลของตนไป ก็จะถูกนำไปใช้ในทางที่ไม่ดีได้ วิธีการแบบนี้เรียกว่า Phishing และก็มีการพัฒนาวิธีการใหม่ๆ ออกมาเพื่อหลอกลวงผู้รับที่รู้ไม่เท่าทันสแปมเมอร์อยู่เสมอ แม้จะใช้มาตรการต่างๆ เพื่อป้องกันและหยุดยั้งสแปมเมลได้มากเพียงใดก็ตาม แต่ก็มีเพียงมาตรการทางกฎหมายเท่านั้น ที่จะสามารถหยุดยั้งการกระทำที่เป็นการละเมิด และหลอกลวงเช่นนี้ได้

4. เพื่อเป็นการวางแนวทางในการทำการตลาดออนไลน์อย่างสแปมเมลให้อยู่ในขอบเขต และไม่เป็นการก้าวละเมิดไปกระทบสิทธิขั้นพื้นฐานของผู้บริโภคในประเทศนั้นอย่างมากมายเกินกว่าขอบเขต

ปัจจุบัน หลายๆ ประเทศทั่วโลกต่างเล็งเห็นความสำคัญของปัญหานี้ และพยายามออกมาตรการทางกฎหมายมาใช้บังคับ และจัดการกับปัญหานี้โดยเฉพาะ เพื่อควบคุมการส่งสแปมเมลให้อยู่ภายในขอบเขต และเชื่อถือได้ ทั้งนี้ มาตรการต่างๆ ที่แต่ละประเทศนำมาใช้ ก็ขึ้นอยู่กับความเหมาะสมตามสภาพสังคม กฎหมาย และแนวคิดของผู้คนในแต่ละประเทศนั่นเอง ทำให้มาตรการทางกฎหมายของแต่ละประเทศมีความเข้มข้นแตกต่างกันไป ดังจะได้นำมาศึกษาเพื่อเป็นแนวคิดของมาตรการในการจัดการกับสแปมเมลในแต่ละประเทศ อันได้แก่ กฎหมายของประเทศสหรัฐอเมริกา อันเป็นประเทศที่มีความก้าวหน้าทางเทคโนโลยีเป็นอันดับหนึ่งของโลก ซึ่งประสบกับปัญหาดังกล่าวมานาน แต่เพิ่งจะมีกฎหมายเฉพาะออกมาบังคับใช้เมื่อไม่นานมานี้ อีกทั้งสหรัฐฯ ยังเป็นแหล่งกำเนิดของสแปมเมล

แหล่งใหญ่ของโลก ดังนั้นความน่าสนใจจึงอยู่ที่ว่า สหรัฐฯ จะมีแนวทางในการจัดการกับปัญหาสแปมเมลในประเทศตนอย่างไร เพื่อลด และควบคุมสแปมเมลในประเทศของตนในอยู่ในปริมาณที่สามารถควบคุมได้

กฎหมายของประเทศในกลุ่มสหภาพยุโรป เนื่องจากประเทศในกลุ่มนี้อันได้แก่ [10] Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, United Kingdom และประเทศสมาชิกของ EFTA คือ Iceland, Liechtenstein, Norway อยู่ภายใต้ข้อตกลงในเรื่องเขตเศรษฐกิจเสรี ดังนั้น EU Directive ทุกฉบับจึงถือเป็นแนวทางที่ต้องผูกพันประเทศสมาชิกเหล่านี้ด้วย ความน่าสนใจจึงอยู่ที่ว่าแนวทางของ EU Directive นั้นเป็นอย่างไร ซึ่งมีผลให้ประเทศสมาชิกต้องออกกฎหมายภายในของตนเพื่อให้สอดคล้องกับแนวทางดังกล่าว

เกาหลีใต้เป็นประเทศในแถบเอเชียที่เป็นต้นกำเนิดของสแปมเมลติดอันดับโลก ทั้งนี้เนื่องจากการเริ่มมีกฎหมายต่อต้านสแปมเมลออกมาบังคับใช้ในสหรัฐฯ และประเทศในกลุ่มยุโรป ทำให้สแปมเมอร์ต้องพยายามหาทางในการส่งสแปมเมลแหล่งใหม่ เพื่อหลีกเลี่ยงกฎหมายที่เข้มงวดในประเทศของตน ประเทศในแถบเอเชียหลายประเทศ จึงเป็นแหล่งที่สแปมเมอร์สนใจในการเข้ามาลักลอบใช้ทรัพยากรของประเทศนั้นเป็นเครื่องส่งสแปมเมล จากปัญหาความรุนแรงที่เพิ่มขึ้นอย่างเหลือเชื่อของปัญหาสแปมเมลในประเทศเกาหลี ทำให้ประเทศต้องหามาตรการใหม่ๆ ออกมาจัดการกับสแปมเมล เกาหลีใต้จึงเป็นประเทศในแถบเอเชียที่น่าสนใจในการศึกษามาตรการต่อต้านสแปมเมล

## 3.4 แนวคิดทางกฎหมายและมาตรการทางกฎหมายกับจัดการกับปัญหาจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงปรารถนาในสหรัฐอเมริกา

### 3.4.1 ประวัติศาสตร์ทางกฎหมายในการแก้ไขปัญหาจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงปรารถนาในสหรัฐอเมริกา

อย่างที่ได้กล่าวมาแล้วข้างต้น สหรัฐฯ เป็นต้นกำเนิดขนาดใหญ่ของสแปมเมลทั่วโลกกว่าร้อยละ 50 แต่รัฐบาลกลางของสหรัฐฯ ก็ยังไม่มีมาตรการทางกฎหมายใดๆ ที่ออกมาบังคับกับเรื่อง

---

[10] http://www.euro.cauce.org/en/countries/index.html

นี้ ทั้งนี้ สภาคองเกรสของสหรัฐฯ ได้มีความพยายามหลายครั้งในการร่างกฎหมายออกมา เพื่อแก้ไขและควบคุมปัญหาเกี่ยวกับสแปมเมลที่ดูจะรุนแรงอย่างต่อเนื่องตั้งแต่ปี 2000 เป็นต้นมา อย่างไรก็ตามความพยายามดังกล่าวดูเหมือนจะยังไม่ประสบความสำเร็จเท่าไรนัก เมื่อเทียบกับมลรัฐต่างๆ มากกว่า 38 มลรัฐ[11]ที่มีกฎหมายที่เกี่ยวข้องกับสแปมเมลประกาศใช้แล้ว ในขณะที่รัฐบาลกลางยังไม่มีการตรากฎหมายใดที่เกี่ยวข้องกับสแปมเมลออกมา รัฐต่างๆ ก็เริ่มที่จะตรากฎหมายที่ห้ามหรือจำกัดความสามารถของพวกสแปมเมอร์เพื่อใช้บังคับภายในรัฐของพวกเขาเองแล้ว ตัวอย่างเช่น[12]

เนวาด้า (Nevada) กลายเป็นรัฐแรกในประเทศ ที่มีการตรากฎหมายที่เกี่ยวข้องกับสแปมในเดือนกรกฎาคมปี 1997 และได้มีการแก้ไขเพิ่มเติมในปี 2001 และ 2003 ภายใต้ประมวลกฎหมายฉบับปัจจุบันของเนวาด้า (NEVADA REVISED STATUTES 2005 - NRS) เรื่องความรับผิดของผู้ส่งอีเมลที่เป็นการโฆษณา (LIABILITY OF PERSONS WHO TRANSMIT ITEMS OF ELECTRONIC MAIL THAT INCLUDE ADVERTISEMENTS) ใน NSR 41.705 ถึง 41.735[13] โดยถือเป็นความผิดในการส่งอีเมลโฆษณา ถ้าไม่มีการจ่าหน้าที่ชัดเจน หรือสามารถแยกแยะได้อย่างทันทีว่าเป็นอีเมลโฆษณา และไม่ปรากฏชื่อผู้ส่ง ที่อยู่ อีเมล พร้อมด้วยวิธีการยกเลิก กฎหมายยังห้ามการส่งสแปมเมลที่มีการให้ข้อมูลผู้ส่งที่ไม่เป็นจริง หรือการขายโปรแกรมที่ออกแบบเพื่อใช้ปลอมแปลงข้อมูลต้นทาง (NSR 205.492) กฎหมายยังให้ผู้รับสแปมเมลฟ้องคดีผู้ส่งถ้าไม่ใช่เป็นการทำธุรกิจกันมาก่อน หรือมีความสัมพันธ์ส่วนตัว หรือผู้รับให้ความยินยอมแคลิฟอร์เนีย (California) ได้ออกกฎหมายเกี่ยวกับสแปมเมลในปี 2003 โดยบัญญัติไว้ใน Part 3, Chapter 1 – Advertising, Article 1.8 - Restrictions On Unsolicited Commercial E-mail Advertisers (17529-17529.9) ของประมวลกฎหมายแคลิฟอร์เนีย (CALIFORNIA BUSINESS AND PROFESSIONS CODE - BPC) และแคลิฟอร์เนียก็เป็นรัฐที่สองที่รับเอาวิธีการให้ความยินยอมบอกรับอีเมลโฆษณา (Opt-in) มาบังคับใช้ สาระสำคัญภายใต้กฎหมายฉบับนี้คือ การส่งออกอีเมลเชิงพาณิชย์โดยไม่ได้ร้องขอ (unsolicited commercial e-mail) จากแคลิฟอร์เนีย หรือส่งถึงที่อยู่อีเมลในแคลิฟอร์เนีย ถือเป็นความผิด (BPC 17529.5.) กฎหมายนี้ยังอนุญาตให้ผู้เสียหาย ผู้ให้บริการอินเตอร์เนต และอัยการรัฐฟ้องสแปมเมอร์ที่

---

[11] http://www.spamlaws.com/state/index.shtml

[12] Smith, R. Eliminating The Spam From Your Internet : the possible effects of the unsolicited commercial electronic mail act of 2001 on junk e-mail . Texas Tech Law Review 35, 411 (2004).

[13] http://www.leg.state.nv.us/NRS/NRS-041.html

ละเมิดบทบัญญัติภายใต้กฎหมายฉบับนี้ด้วย (BPC 17529.8.) อย่างไรก็ดี การห้ามที่กว้างของกฎหมายฉบับนี้ ได้เป็นที่วิพากษ์วิจารณ์อย่างมากถึงความชอบด้วยรัฐธรรมนูญของสหรัฐฯ ซึ่งคดี Ferguson v. Friendfinders ที่จะได้กล่าวถึงต่อไปก็ได้สนับสนุนถึงความถูกต้องตามรัฐธรรมนูญของกฎหมายฉบับนี้

วอชิงตัน (Washington) ได้ออกกฎหมายที่เกี่ยวกับสแปมเมล ในเดือนมีนาคมปี 1998 และแก้ไขในเดือนพฤษภาคม ปี 1999 ซึ่งปรากฏอยู่ใน Title 19 - Business regulations - miscellaneous, chapter 19.190 – Commercial electronic mail ประมวลกฎหมายฉบับแก้ไขของวอชิงตัน (Revised Code of Washington - RCW) โดยถือเป็นการละเมิดกฎหมายคุ้มครองผู้บริโภค หากมีการส่งข้อความอีเมลเชิงพาณิชย์โดยใช้ชื่อโดเมนเนม (Domain Name)* ของบุคคลที่สามโดยไม่ได้รับอนุญาต หรือข้อมูลต้นทางอีเมลหายไปหรือไม่ถูกต้อง หรือใช้หัวข้ออีเมลที่ผิดหรือก่อให้เกิดความเข้าใจผิด (RCW 19.190.030.) กฎหมายนี้ใช้บังคับกับการส่งอีเมลออกไปจากรัฐวอชิงตัน หรือในกรณีที่ผู้ส่งสามารถทราบได้ว่าผู้รับเป็นพลเมืองของรัฐวอชิงตัน หรือได้รับการยืนยันจากผู้จดทะเบียนโดเมนเนมที่ปรากฏอยู่บนที่อยู่อีเมลของผู้รับว่าผู้รับเป็นพลเมืองของวอชิงตัน กฎหมายฉบับนี้ได้ถูกนำมาใช้กล่าวอ้างในคดี State v. Heckel ซึ่งศาลสูงวอชิงตันถือว่ากฎหมายการต่อต้านสแปมไม่ได้ละเมิดบทบัญญัติรัฐธรรมนูญแต่อย่างใด ดังจะได้กล่าวถึงรายละเอียดต่อไป

เวอร์จิเนีย (Virginia) ซึ่งเป็นรัฐที่เต็มไปด้วยสแปมเมอร์นั้น ตามลายลักษณ์อักษรแล้วเวอร์จิเนียมีกฎหมายต่อต้านสแปมที่ไม่แตกต่างจากกฎหมายของรัฐอื่นๆ เป็นพิเศษแต่อย่างใด แต่จากการแก้ไขเพิ่มเติมเมื่อกรกฎาคม 2003 นี้ ทำให้เวอร์จิเนียมีกฎหมายที่สนับสนุนรัฐอย่างกว้างขวางมากที่สุดในการต่อต้านสแปมในสหรัฐฯ จากประมวลกฎหมายของเวอร์จิเนีย (VIRGINIA CODE) Title 18.2. - Crimes and offenses generally, Chapter 5 – Crimes against property, Sections 18.2 - 152.2, 152.3:1, 152.4, 152.12 (2003) สาระสำคัญของกฎหมายฉบับนี้คือ การกำหนดบทลงโทษเพื่อต่อต้านสแปมเมอร์ โดยจะกลายเป็นความผิดทางอาญา และอนุญาตให้จำคุกเป็นระยะเวลา 1-5 ปี สำหรับผู้ที่ส่งสแปมอีเมลมากกว่า 10,000 ฉบับต่อวัน หรือ 100,000 ฉบับในช่วงระยะเวลา 30 วัน และมี

---

* โดเมนเนม (Domain Name) เป็นชื่อสำหรับเรียกชื่อที่อยู่ของเวบเพจ (web page) หรือ โฮมเพจ (home page) ซึ่งแต่เดิมถูกระบุโดยใช้ตัวเลขแทน เช่น 203.121.145.95 เป็นต้น โดเมนเนมยังสามารถเรียกแทนด้วยชื่ออื่นอีกหลายชื่อ ซึ่งจะมีความหมายคล้ายกัน คือ เวบไซต์ (web site) ยูอาร์แอล (URL) หรือ โฮมเพจ (home page) ปัจจุบันชื่อโดเมนที่นิยมจดทะเบียนจะมีนามสกุลเป็น ".COM" เพราะเป็นที่รู้จักแพร่หลายมากกว่า

รายได้ที่ได้รับจากการส่งสแปมเมลเพียงครั้งเดียวมีจำนวนมากกว่า 1,000 เหรียญดอลล่าห์สหรัฐฯ, หรือรวมกันทั้งหมดมากกว่า 50,000 เหรียญดอลล่าห์สหรัฐฯ นอกจากนั้น ถ้ามีการจ้างผู้เยาว์ให้เป็นผู้ช่วยในการส่งสแปมเมล ก็จะถือเป็นความผิดอาญาด้วยเช่นกัน (§ 18.2-152.3:1.) การใช้วิธีที่รุนแรงแบบใหม่เพื่อกำจัดสแปมนี้เกิดขึ้นจากความจริงที่ว่า ทราฟฟิคบนอินเตอร์เนตของสหรัฐอเมริกามากกว่า 50% ต้องวิ่งผ่านรัฐเวอร์จิเนียบางส่วน เพราะว่าผู้ให้บริการรายใหญ่ที่สุดของสหรัฐฯ หรือ American Online (AOL) ตั้งอยู่ที่นั่น โดยกฎหมายใหม่ฉบับนี้ยังยอมให้ศาลรัฐเวอร์จิเนียใช้เขตอำนาจศาลเหนือบุคคลเพื่อให้สามารถเข้าถึงสแปมเมอร์ที่ตั้งอยู่ในรัฐอื่น ถ้ามีจุดคาบเกี่ยวใดตามที่บัญญัติไว้ในประมวลกฎหมายของเวอร์จิเนีย (VIRGINIA CODE) Title 8.01. Civil remedies and procedure, Chapter 9. Personal jurisdiction in certain actions, Sections 8.01-328.1. ซึ่งเป็นที่วิพากษ์วิจารณ์ว่ากฎหมายฉบับนี้ นอกจากจะก่อให้เกิดคำถามในเรื่องเขตอำนาจศาลที่น่าจะเป็นอุปสรรคต่อกรณีเหล่านั้นแล้ว ยังไม่น่าจะได้รับความร่วมมืออย่างดีจากเจ้าหน้าที่จากรัฐอื่นๆ ด้วย

แม้ว่าแต่ละรัฐจะพยายามออกกฎหมายของตนเองมาต่อสู้กับสแปมเมลในสหรัฐฯ แต่กฎหมายเหล่านั้น ก็ไม่ประสบผลสำเร็จเท่าที่ควร ทั้งนี้ เนื่องจาก

1. กฎหมายเหล่านี้ส่วนมากมักไม่ได้รับการยอมรับ ภายใต้บทบัญญัติรัฐธรรมนูญแห่งสหรัฐฯ เพราะการออกกฎในเรื่องที่เกี่ยวกับอีเมล อันเป็นเป็นอิสระจากที่อยู่ทางภูมิศาสตร์นั้น เป็นเรื่องที่ละเอียดอ่อนอย่างมาก เนื่องจากว่าเวลาผู้ส่ง ส่งสแปมเมลนั้น ผู้ส่งไม่ได้คำนึงถึงว่าผู้รับอยู่ในรัฐใดหรืออาจทราบได้ว่าผู้รับอยู่รัฐใด อันควรจะต้องเรียนรู้และปรับใช้กฎหมายของรัฐนั้นก่อนส่งสแปมเมลหรือไม่

2. กฎหมายต่อต้านสแปมเมลในแต่ละรัฐมีความแตกต่างกันในรายละเอียด ซึ่งพลเมืองที่ต้องปฏิบัติตามกฎหมายเหล่านั้น อาจรู้สึกสับสนได้ว่ากฎหมายของรัฐใดที่พวกเขาจะต้องนำมาปฏิบัติตาม เพราะที่อยู่อีเมลนั้นไม่อาจเจาะจงที่อยู่ทางภูมิศาสตร์ของผู้รับได้ หากส่งอีเมลออกไปโดยที่ไม่ได้ปรับใช้กฎหมายที่เหมาะสม ก็อาจถือเป็นการกระทำที่ผิดกฎหมายของรัฐนั้นได้

3. ปัญหาที่เห็นได้ชัดอีกประการหนึ่งคือ เขตอำนาจศาลของแต่ละรัฐในการจัดการกับสแปม อย่างที่ทราบกันดีว่า สหรัฐฯ นั้นมีระบบการปกครองแบบสหพันธรัฐ ดังนั้น ผู้ที่อยู่อาศัยในรัฐใด ก็ปรับใช้กฎหมายของรัฐที่ตนเองอยู่นั้น กับการกระทำที่เกิดขึ้น แต่การขาดซึ่งเขตแดนทางภูมิศาสตร์ในไซเบอร์สเปซเป็นปัญหาที่สำคัญในการจัดการอินเตอร์เนตทั้งในระดับรัฐ ระดับชาติและในทางระหว่างประเทศ ไม่เหมือนกับโลกแห่งความจริง (real world) ที่มีขอบเขตทางภูมิศาสตร์เป็น

เสมือนรั้วกั้น อันก่อให้เกิดการบัญญัติและการบังคับใช้กฎหมาย ในขณะที่ไซเบอร์สเปซเป็นเสมือนของเหลว ที่มีอยู่ในทุกหนทุกแห่ง และขาดซึ่งความมีอาณาเขตที่จะกำหนดประเด็นเรื่องเกี่ยวกับเขตอำนาจศาลในการเลือกกฎหมายและศาลให้มีคำพิพากษาเพื่อแก้ไขข้อขัดแย้งได้

จากปัญหาของรัฐในการออกกฎหมาย ดังที่กล่าวมานี้เอง ทำให้รัฐบาลกลางพยายามหามาตรการทางกฎหมายออกมาใช้แก้ไขปัญหาสแปมเมลในสหรัฐฯ เพื่อให้มีมาตรฐานเดียวกันทั้งประเทศ และไม่ก่อให้เกิดความขัดแย้งระหว่างรัฐด้วยกันเองในการปรับใช้กฎหมาย อย่างไรก็ดี การบัญญัติกฎหมายต่อต้านสแปมเมลก็ไม่ใช่เรื่องง่าย ทั้งการผสมผสานมาตรการที่มีอยู่ในแต่ละรัฐให้เป็นที่ยอมรับมากที่สุด และยังต้องเผชิญกับบทบัญญัติตามรัฐธรรมนูญอีก กฎหมายของรัฐบาลกลางจึงใช้เวลาค่อนข้างนาน กว่าจะผ่านสภาคองเกรซมาได้

3.4.2 ความเป็นมาของกฎหมายต่อต้านสแปมเมลในสหรัฐอเมริกา (CAN SPAM Act of 2003)

สหรัฐฯ ได้มีความพยายามในการเสนอร่างกฎหมายเพื่อควบคุมสแปมเมลมาตั้งแต่ปี 1999 แต่กฎหมายทั้งหมดก็ไม่ผ่านรัฐสภาของสหรัฐฯ[14] และได้มีความพยายามเสนอกฎหมายต่อต้านสแปมเมลเรื่อยมา แต่ก็ไม่ประสบผลสำเร็จ จนกระทั่งปี 2003 กฎหมายเพื่อจัดการกับสแปมเมลฉบับแรกก็ผ่านสภา และได้ตราออกมาเป็นกฎหมาย มีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2004 เป็นต้นไป เหตุผลที่ทำให้การออกกฎหมายมีความล่าช้า ก็เนื่องจากการออกกฎหมายในเรื่องที่เกี่ยวกับอินเตอร์เนตนั้นเป็นเรื่องที่ยาก และละเอียดอ่อน เพื่อที่จะทำอย่างไรให้สามารถขจัดการฉ้อโกง หลอกลวงต่างๆ ผ่านทางสแปมเมล โดยอันที่จะไม่กระทบกระเทือนถึงเสรีภาพในเชิงพาณิชย์[15] นอกจากนั้น ความคิดเห็นที่ขัดแย้งกันของหลายๆ ฝ่ายก็เป็นเหตุที่ทำให้การออกกฎหมายต่อต้านสแปมเมลต้องล่าช้าออกไปอีกด้วย ซึ่งฝ่ายที่คัดค้านการออกกฎหมายฉบับนี้ ก็มีทั้งที่คัดค้านอย่างที่สุด เพราะกลัวว่าการออกกฎหมายหรือการควบคุมเช่นนั้น จะก่อให้เกิดผลกระทบต่อสิทธิในการแสดงความคิดเห็น

---

[14] David E. Sorkin, "Proposed legislation," at http://www.spamlaws.com/federal/index.shtml (last visited February 2006).

[15] House of Commons Select Committee on Adulteration of Foods, Drinks and Drugs, Third Report, 1856, 56-7, at 253; John Abraham, Science, Politics and the Pharmaceutical Industry: Controversy and Bias in Drug Regulation 41 (1995) Cited in Taiwo A. Oriola, "Regulating Unsolicited Commercial Electronic Mail in the United States and the European Union: Challenges and Prospects," 7 Tul. J. Tech. & Intell. Prop. 113 (2005).

(Freedom of speech) ในขณะที่อีกฝ่ายสนับสนุนการออกกฎของตัวเอง หรือมาตรการการจัดการทางเทคนิคสำหรับไซเบอร์สเปซ เพราะกลัวว่าการมีบทบัญญัติทางกฎหมายนั้น จะเป็นการควบคุมสถานการณ์ และไม่สามารถที่จะขับเคลื่อนให้เกิดสิ่งใหม่ๆ อันจะนำมาซึ่งความก้าวหน้าทางเทคโนโลยีอย่างรวดเร็วอย่างที่อินเตอร์เนตทุกวันนี้เป็นได้ อย่างไรก็ตาม ความเป็นจริงก็คือว่าการจัดการกับปัญหาที่เกี่ยวข้องกับอินเตอร์เนตนั้นต้องผสมผสานระหว่างการออกข้อบังคับ นโยบาย และเงื่อนไข (Condition & Policy) ในการใช้อินเตอร์เนต, มาตรการการควบคุมทางเทคนิค, และการออกกฎหมายของรัฐเข้าด้วยกัน ดังนั้น ความท้าทายจริงๆ ในระยะยาว คือทำอย่างไรจึงจะเป็นวิธีที่ดีที่สุดที่จะจัดให้พร้อมซึ่งกลยุทธ์ทั้งสามอันนี้ให้ยับยั้งสแปมเมลได้อย่างมีประสิทธิภาพ

CAN SPAM Act of 2003 (The Controlling the Assault of Non – Solicited Pornography and Marketing Act of 2003) นี้ถูกเสนอโดยวุฒิสมาชิก Conrad R. Burns และ Ron Wyden เมื่อเดือนเมษายน 2003 ซึ่งเป็นร่างกฎหมายที่เปลี่ยนแปลงเพียงเล็กน้อยเท่านั้นจากร่างเดิมเมื่อปี 2002 โดยรวมเอาเนื้อหาบางส่วนของ Criminal Spam Act of 2003 และ Stop Pornography and Abusive Marketing Act เข้าไว้ใน CAN SPAM Act of 2003 ด้วย หลังจากผ่านการพิจารณาจากวุฒิสมาชิก และสภาผู้แทนฯ เมื่อเดือนพฤศจิกายน และธันวาคม 2003 ตามลำดับ CAN SPAM Act of 2003 ก็ได้ตราเป็นกฎหมายโดยประธานาธิบดีบุชเมื่อวันที่ 16 ธันวาคม 2003 โดยให้เริ่มมีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2004 เป็นต้นมา

วัตถุประสงค์ในการตรากฎหมายฉบับนี้ก็เนื่องจากสภาคองเกรซพบว่า[16]

(1) จดหมายอิเล็กทรอนิกส์ (Email) ได้กลายเป็นสิ่งสำคัญและเป็นวิธีการสื่อสารที่ได้รับความนิยมอย่างมาก จากประชนชาวอเมริกันเพื่อวัตถุประสงค์ส่วนตัว และเพื่อการพาณิชย์ เพราะมีค่าใช้จ่ายถูก และสามารถเข้าถึงได้ทั่วโลก ซึ่งทำให้เกิดความสะดวกสบาย และมีประสิทธิภาพอย่างมาก และยังเสนอโอกาสโดยเฉพาะในการพัฒนา และการเติบโตของการพาณิชย์ที่ตรงไปตรงมา

(2) ความสะดวก และความมีประสิทธิภาพของอีเมลนั้น ถูกคุกคามโดยการเติบโตอย่างรวดเร็วของปริมาณจดหมายอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอ ซึ่งสันนิษฐานว่ากินพื้นที่

---

[16] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C.A. 7701-7713 (Supp. VI 2004).

มากกว่าครึ่งของทราฟฟิคอีเมลทั้งหมด ซึ่งเพิ่มขึ้นจากการประมาณการในปี 2001 ถึง 7 เปอร์เซ็นต์ และมีปริมาณเพิ่มขึ้นอย่างต่อเนื่อง ซึ่งอีเมลเหล่านี้ส่วนใหญ่นั้นมีลักษณะฉ้อโกง และหลอกลวง

(3) การได้รับจดหมายอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอเหล่านี้อาจจะเป็นผลให้เกิดค่าใช้จ่ายแก่ผู้รับที่ไม่สามารถปฏิเสธที่จะรับอีเมลเช่นนั้น และต่อผู้ที่มีค่าใช้จ่ายในการเก็บรักษาอีเมลเช่นนั้น หรือเวลาที่ต้องใช้ไปในการเข้าถึง, การตรวจสอบ, และการกำจัดเมลเช่นนั้น หรือ ทั้งสองกรณี

(4) การได้รับข้อความที่ไม่ต้องการจำนวนมหาศาลลดความสะดวกสบายของอีเมล และก่อให้เกิดความเสี่ยงกับข้อความอีเมลที่ต้องการ ทั้งเชิงพาณิชย์ และไม่ใช่ จะสูญหาย ถูกมองข้าม และถูกลบทิ้งไปท่ามกลางปริมาณของข้อความที่ไม่ต้องการจำนวนมาก ดังนั้น จึงเป็นการลดความน่าเชื่อถือ และความมีประโยชน์ของอีเมลต่อผู้รับ

(5) อีเมลเชิงพาณิชย์บางอย่างประกอบไปด้วยเนื้อหาที่ผู้รับจำนวนมากอาจจะพิจารณาว่าหยาบคาย หรือลามกโดยธรรมชาติ

(6) การเติบโตของอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอนำมาซึ่งต้นทุนที่เป็นค่าใช้จ่ายอย่างมากต่อผู้ให้บริการการเข้าถึงอินเตอร์เนต, ธุรกิจ, องค์กรไม่แสวงหากำไร และสถาบันการศึกษาที่ต้องแบก และรับเมลเช่นนั้นไว้ เพราะว่ามีจำนวนของเมลที่จำกัดที่ผู้ให้บริการ, ธุรกิจ และสถาบันต่างๆ สามารถจัดการได้โดยไม่ต้องลงทุนขั้นพื้นฐานเพิ่มเติม

(7) ผู้ส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอจำนวนมากปิดบังแหล่งที่มาของเมลเหล่านั้นโดยเจตนา

(8) ผู้ส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอจำนวนมากใส่ข้อมูลที่นำไปสู่การเข้าใจผิดในหัวข้อของอีเมลโดยเจตนา เพื่อที่จะชักจูงผู้รับให้เปิดดูข้อความ

(9) ขณะที่ผู้ส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอบางรายจัดให้มีวิธีที่ง่าย และเชื่อถือได้สำหรับผู้รับ ที่ต้องการปฏิเสธการรับอีเมลเชิงพาณิชย์จากผู้ส่งเช่นนั้นในอนาคต (หรือที่เรียกว่าวิธี Opt-out) ผู้ส่งบางรายก็ไม่จัดให้มีเครื่องมือเช่น Opt-out หรือไม่มีความซื่อตรงต่อคำร้องขอของผู้รับที่จะไม่รับอีเมลจากผู้ส่งเช่นนั้นในอนาคต หรือทั้งสองกรณี

(10) ผู้ส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอจำนวนมากใช้โปรแกรมคอมพิวเตอร์ในการรวบรวมที่อยู่อีเมลจำนวนมากโดยอัตโนมัติจากเวปไซท์อินเตอร์เนต หรือบริการออนไลน์ที่ผู้ใช้ต้องทิ้งที่อยู่ของพวกเขาไว้เพื่อที่จะทำให้ใช้เวปไซท์ หรือบริการได้เต็มที่

(11) หลายรัฐได้บัญญัติกฎหมายโดยตั้งใจที่จะออกกฎ หรือลดจำนวนอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอ แต่บทบัญญัติเหล่านี้กำหนดให้มีมาตรฐาน และความต้องการที่แตกต่างกัน ซึ่งทำให้แต่ละรัฐไม่ประสบผลสำเร็จในการจัดการกับปัญหาที่เกี่ยวข้องกับอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอ เนื่องจากอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอนั้นมีลักษณะที่ไม่สามารถระบุแหล่งที่มาทางภูมิศาสตร์ได้ จึงเป็นการยากสำหรับธุรกิจที่เคารพกฎหมายที่จะทราบว่ากฎหมายที่แตกต่างกันเหล่านี้ มีฉบับใดที่พวกเขาต้องปฏิบัติตามบ้าง

(12) ปัญหาที่เกี่ยวกับการเติบโตอย่างรวดเร็ว และการคุกคามของอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอไม่สามารถแก้ไขได้โดยกฎหมายของรัฐบาลกลางเท่านั้น การพัฒนา และการรับเอาวิธีการทางเทคนิค และการแสวงหาความพยายามร่วมกันกับประเทศอื่นๆ ก็เป็นสิ่งจำเป็นเช่นเดียวกัน

การตัดสินใจของสภาคองเกรซในนโยบายสาธารณะ บนพื้นฐานของปัญหาดังที่ได้กล่าวมาแล้ว สภาคองเกรซจึงเห็นว่า

(1) มีผลประโยชน์ของรัฐบาลที่มีความจำเป็นในการออกกฎหมายอีเมลเชิงพาณิชย์บนหลักการโดยทั่วไป

(2) ผู้ส่งอีเมลเชิงพาณิชย์ไม่ควรจะทำให้ผู้รับเข้าใจผิดถึงแหล่งที่มา หรือเนื้อหาของเมลเช่นนั้น และ

(3) ผู้รับอีเมลเชิงพาณิชย์ มีสิทธิปฏิเสธที่จะรับอีเมลเชิงพาณิชย์เพิ่มเติมจากแหล่งที่มาเดียวกัน

ดังนั้น จึงได้ตรากฎหมายฉบับนี้ขึ้น เพื่อที่จะวางระเบียบการค้าระหว่างรัฐขึ้น โดยการกำหนดให้มีข้อจำกัด และบทลงโทษ ในการส่งจดหมายอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอ ผ่านทางอินเตอร์เนต

3.4.3 มาตรการทางกฎหมายของ CAN SPAM Act of 2003

The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) ตราขึ้นมาเพื่อบังคับใช้กับผู้ส่งอีเมลเชิงพาณิชย์ มีการแจกแจงโทษสำหรับสแปมเมอร์ และบริษัทที่เป็นเจ้าของสินค้าที่โฆษณาผ่านสแปม ถ้าหากว่าละเมิดกฎหมาย และให้ผู้บริโภคที่สิทธิขอร้องผู้ส่งอีเมลให้หยุดการส่งสแปมเมลถึงพวกเขาด้วย

คณะกรรมการการค้ากลาง หรือ The Federal Trade Commission (FTC) ซึ่งเป็นหน่วยงานในการคุ้มครองผู้บริโภคแห่งชาติ เป็นหน่วยงานที่มีอำนาจบังคับใช้ CAN-SPAM Act. (sec. 7 (a) (d)) และ CAN-SPAM ยังให้กระทรวงยุติธรรม Department of Justice (DOJ) เป็นผู้มีอำนาจในการบังคับใช้มาตรการลงโทษทางอาญาของตัวเองอีกด้วย (sec. 4 (c)(2)) ส่วนหน่วยงานของรัฐบาลกลาง หรือหน่วยงานของรัฐอื่นๆ สามารถบังคับใช้กฎหมายต่อผู้ละเมิดภายใต้เขตอำนาจศาลของพวกเขาได้ (sec. 7 (b)) และยังยอมให้บริษัทที่ให้บริการการเข้าอินเตอร์เนตสามารถฟ้องผู้ละเมิดได้เช่นเดียวกัน (sec. 7 (g))

พระราชบัญญัติฉบับนี้ มีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2004 บังคับใช้กับอีเมลที่มีวัตถุประสงค์เบื้องต้นเพื่อการโฆษณา หรือการส่งเสริมการขายสินค้าหรือบริการในเชิงพาณิชย์ (Unsolicited Commercial E-mail) ซึ่งรวมถึงเนื้อหาของเวปไซต์ด้วย ภายใต้บทบัญญัติของกฎหมายฉบับนี้ โดยเงื่อนไขหลักของกฎหมาย ถือเป็นการฝ่าฝืนหากใครก็ตามที่

(1) ส่งข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ที่ประกอบด้วย หรือแนบมากับข้อมูลจั่วหัวที่ผิดอย่างจงใจ หรือก่อให้เกิดความเข้าใจผิด (false or misleading header information) ซึ่งในอีเมลของผู้ส่งที่ระบุที่มาของอีเมล เช่น มาจากใคร หรือถึงใคร รวมถึงข้อมูลเบื้องต้นอื่นๆ เช่น โดเมนเนมของผู้ส่ง และที่อยู่อีเมล ต้องถูกต้องแท้จริง และระบุได้ถึงบุคคลผู้ทำการส่งอีเมล (sec. 5 (a)(1))

(2) ส่งอีเมลเชิงพาณิชย์ด้วยข้อความหัวเรื่อง ที่น่าจะทำให้เกิดความเข้าใจผิดแก่ผู้รับ ว่าอะไรคือเนื้อหาที่แท้จริงของข้อความ (deceptive subject lines) โดยในบรรทัดหัวข้ออีเมลต้องไม่ทำให้ผู้รับเกิดความเข้าใจผิดเกี่ยวกับเนื้อหา หรือสาระที่สำคัญของข้อความ (sec. 5 (a)(2))

(3) ส่งอีเมลเชิงพาณิชย์ที่ไม่มีการทำงาน และที่อยู่อีเมลกลับที่แสดงให้เห็นอย่างชัดเจน หรือกลไกโต้ตอบทางอินเตอร์เนตอื่นๆ ที่อนุญาตให้ผู้รับส่งคำร้องขอที่จะไม่รับอีเมลเหล่านี้ได้

ในอนาคตถึงที่อยู่อีเมลของผู้ส่งนั้น (an opt-out method) และผู้ส่งต้องซื่อสัตย์ต่อคำร้องขอนั้นด้วย โดยอาจจะสร้างเมนูเพื่อเป็นทางเลือกแก่ผู้รับในการยกเลิกการรับข้อความเช่นนั้นอีก และต้องมีทางเลือกนั้นในตอนท้ายของข้อความเชิงพาณิชย์ใดๆ จากผู้ส่งเสมอ (sec. 5 (a)(3))

กลไกในการยกเลิก ที่ผู้ส่งเสนอมาใดๆ ก็ตามต้องใช้งานได้ไม่น้อยกว่า 30 วัน หลังจากที่อีเมลต้นกำเนิดถูกส่ง เมื่อผู้ส่งได้รับคำร้องขอที่จะไม่รับอีเมลเหล่านั้นแล้ว ผู้ส่งต้องหยุดการส่งอีเมลถึงที่อยู่อีเมลของผู้ร้องขอภายใน 10 วัน โดยผู้ส่งไม่สามารถช่วยผู้มีสิทธิอื่นส่งอีเมลถึงที่อยู่อีเมลนั้น หรือใช้สิทธิของผู้อื่นส่งอีเมลนั้นในนามของตนถึงที่อยู่อีเมลนั้น และยังถือว่าเป็นการกระทำที่ผิดกฎหมายในกรณีที่ผู้ส่งขาย หรือถ่ายโอนที่อยู่อีเมลของบุคคลที่เลือกที่จะไม่รับอีเมลของตน แม้แต่ในรูปของบัญชีส่งเมล (Mailing list) (sec. 5 (a)(4))

(4) ผู้ใดที่ส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอ โดยไม่จัดให้มีสิ่งเหล่านี้ ถือเป็นการกระทำผิดกฎหมายด้วย (sec. 5 (a)(5))

(1) สิ่งบ่งชี้ที่เห็นได้ชัด และชัดแจ้ง ว่าข้อความนั้นเป็นการโฆษณา หรือการชักชวน (identified as an advertisement) หรือมีสินค้าโฆษณาที่มีจุดมุ่งหมายในเรื่องเพศ

(2) ข้อสังเกตที่เห็นได้ชัดเจน และไม่คลุมเครือถึงโอกาสที่จะปฏิเสธที่การรับอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอเพิ่มเติม (clear and conspicuous notice) ในอนาคตได้

(3) ที่อยู่ทางไปรษณีย์ที่สมบูรณ์ของผู้ส่ง (sender's valid physical postal address)

การละเมิดบทบัญญัติดังกล่าวข้างต้นนั้นจะถูกปรับ 11,000 เหรียญดอลล่าห์สหรัฐ หรือมากกว่านั้น และอาจถูกปรับเพิ่มเติมได้ ถ้าหากว่าผู้ส่งอีเมลเชิงพาณิชย์ไม่เพียงแต่ละเมิดบทบัญญัติข้างต้นเท่านั้น แต่ยังรวมถึง (sec. 5 (b)(1))

(1) การเก็บเกี่ยวที่อยู่อีเมลจากเวปไซท์ หรือเวปเซอร์วิสที่แสดงข้อห้ามในการถ่ายโอนที่อยู่อีเมล

(2) การสร้างที่อยู่อีเมลโดยการใช้วิธี "dictionary attack" คือการผสมชื่อ, ตัวอักษร, ตัวเลข โดยการเปลี่ยนรูปไปหลายแบบ

(3) ใช้ต้นแบบ หรือวิธีอัตโนมัติอื่นๆ เพื่อลงทะเบียนใช้อีเมล หรือบัญชีผู้ใช้ (user accounts) หลายๆ แห่ง เพื่อใช้ส่งอีเมลเชิงพาณิชย์

(4) ทยอยส่งอีเมลผ่านคอมพิวเตอร์หรือเครือข่ายโดยไม่ได้รับอนุญาต ตัวอย่างเช่น โดยการอาศัยข้อได้เปรียบจากการเปิด relay หรือการเปิด proxies โดยไม่มีอำนาจ

กฎหมายยังยอมให้กระทรวงยุติธรรมเสาะหาโทษทางอาญา รวมถึงการจำคุก สำหรับผู้ส่งอีเมลเชิงพาณิชย์ที่ทำการ หรือร่วมกันทำการ (sec. 4 (a))

(1) ใช้คอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจ และส่งอีเมลเชิงพาณิชย์จาก หรือโดยผ่านคอมพิวเตอร์เครื่องนั้น

(2) ใช้คอมพิวเตอร์ในการส่งผ่าน หรือส่งซ้ำไปซ้ำมาซึ่งอีเมลเชิงพาณิชย์ เพื่อหลอกลวง หรือทำให้ผู้รับหรือผู้ให้บริการการเข้าถึงอินเตอร์เนตเข้าใจผิด ในต้นทางของข้อความนั้น

(3) ให้ข้อมูลจั่วหัวที่ผิดในข้อความอีเมลหลายฉบับ และริเริ่มส่งข้อความเช่นนั้น

(4) ลงทะเบียนใช้บัญชีอีเมลหลายอัน หรือโดเมนเนมใช้ข้อมูลที่ผิดในการระบุตัวผู้ส่งทะเบียนที่แท้จริง

(5) แสดงตนอย่างผิด ว่าเป็นเจ้าของที่อยู่ Internet Protocol หลายอันที่ใช้ในการส่งข้อความอีเมลเชิงพาณิชย์

FTC จะออกมาตรการเพิ่มเติมภายใต้ CAN-SPAM Act ที่เกี่ยวข้องกับการขอให้มีข้อความบ่งบอกถึงอีเมลเชิงพาณิชย์ที่เกี่ยวกับเพศ และหลักเกณฑ์เบื้องต้นในการจำกัดความของคำว่า "วัตถุประสงค์ขั้นต้น" (the primary purpose) ของอีเมลเชิงพาณิชย์ โดยการออกมาตรการเหล่านี้ต้องทำให้เสร็จภายในสิ้นปี 2004 กฎหมายยังกำหนดให้ FTC รายงานต่อสภาคองเกรซในช่วงกลางปี 2004 ในเรื่องที่จะจัดให้มีการลงทะเบียนห้ามการส่งสแปมเมลแห่งชาติได้ (Do-Not-Email registry) และให้ออกรายงานภายใน 2 ปีถัดไปในเรื่องการบ่งชี้ถึงประเภทของอีเมล, การสร้างระบบรองรับในการบังคับใช้กฎหมาย และความมีประสิทธิภาพ และการบังคับใช้ CAN-SPAM Act. (sec. 9, 10, 13)

ในเดือนเมษายน 2004 เจ้าหน้าที่ของรัฐบาลกลางได้เริ่มฟ้องคดีอาญาเป็นครั้งแรกภายใต้ CAN-SPAM Act ใน FTC v. Phoenix Avatar LLC, และ United States v. Lin. FTC กล่าวหา Phoenix Avatar LLC และตัวแทนที่ตั้งอยู่ที่ Detroit สำหรับข้อกล่าวหาว่า การหลั่งไหลเข้าไปใน

อินเตอร์เนตจำนวนมากซึ่งเกือบจะครึ่งล้านข้อความอีเมล ใน Lin[17] เอกสารคำฟ้องแสดงว่าจำเลยโดยถูกกล่าวหาว่าใช้การเป็นเท็จและการหลอกลวงที่จะซ่อนถึงต้นกำเนิดข้อความสแปมของพวกเขา และปิดบังถึงความมีตัวตนของพวกเขาโดยการใช้ที่อยู่อีเมลของบุคคลที่สามที่ไม่รู้เรื่องด้วย พวกเขายังได้ขายแผ่นปะลดน้ำหนักอันหลอกลวงซึ่งพวกเขาสามารถทำเงินได้เกือบจะ 100,000 ดอลล่าห์ต่อเดือนจากการขายสินค้า

3.4.4 ความคาดหวังต่อความมีประสิทธิภาพในการบังคับใช้ CAN SPAM Act of 2003

อย่างที่ได้กล่าวไว้ในตอนต้นว่า ความท้าทายอย่างมากต่อมาตรการต่อต้านสแปมคือการควบคุมความสมดุลในผลประโยชน์ที่ขัดแย้งกัน ระหว่างสิทธิของผู้ส่งสแปมที่จะส่งข้อความเชิงพาณิชย์ที่ไม่ได้ร้องขอ (ซึ่งกว้างกว่าเรื่องการพูดโดยอิสระ) และสิทธิของผู้รับสแปมในเรื่องความเป็นส่วนตัว (ซึ่งมีลักษณะเช่นเดียวกับเรื่องการพูดการอิสระด้วย) แน่นอนว่ามีเส้นแบ่งอย่างชัดเจนระหว่างสิทธิที่ขัดแย้งกันเหล่านี้บนมุมมองทางรัฐธรรมนูญ ที่เต็มไปด้วยความคิดทางกฎหมาย การกระทำให้เกิดความสมดุลที่ต้องอาศัยความละเอียดอ่อนเช่นนี้ปรากฏอยู่ทั่วๆ ไป ในบทบัญญัติของ the CAN-SPAM Act ตัวอย่างเช่น แม้ว่าสภาคองเกรซพบว่าอีเมลเชิงพาณิชย์นั้นมีการผสมผสานกันของภาพลามกและการหลอกลวง หรือบ่อยครั้งมีการใช้หัวข้ออีเมลที่ก่อให้เกิดความเข้าใจผิด เพื่อให้จูงใจผู้รับในการอ่านอีเมลที่ไม่ได้ร้องขอ ถึงกระนั้นก็ดี กฎหมายนี้ ก็ยังยอมให้มีวิธี เช่น "opt-out" อันเป็นวิธีการไม่ให้ความยินยอมในการส่งอีเมลในอนาคต ซึ่งนักวิเคราะห์หลายคนเชื่อว่าเป็นการให้สแปมเมอร์มีความได้เปรียบมากขึ้น อย่างไรก็ตามกฎหมายที่มีความสมดุลนี้ ได้ก่อให้เกิดความยุติธรรมที่จะนำมาปรับใช้กับนักการตลาดทางอินเตอร์เนตที่ถูกกฎหมาย ซึ่งทำให้การส่งโฆษณาลดน้อยลงโดยวิธี "opt-in" ทำให้ผู้รับสแปมเมลควบคุมได้มากขึ้นตามลำดับว่าสแปมอะไรที่จะหมาะสมต่อกล่องจดหมายของพวกเขา

อย่างไรก็ตาม กฎหมายนี้ก่อให้เกิดการวิพากษ์จากบุคคลทั่วไปที่เกี่ยวข้องว่า[18] มี ความอ่อนแอเกินไปในการต่อสู้กับสแปม ในขณะที่ได้รับเสียงวิจารณ์ว่า กฎหมายฉบับนี้ละเมิดการพูดอย่าง

---

[17] Feds Charge Four Under New Anti-Spam Law, Andrews Computer & Internet Litig. Rep. (Andrews Publications, Wayne, PA), May 18, 2004, at 9.

[18] Taiwo A. Oriola, "Regulating Unsolicited Commercial Electronic Mail in the United States and the European Union: Challenges and Prospects," Tulane Journal of Technology & Intellectual Property 7, 113 (spring 2005) : 6-7.

มีอิสระตามรัฐธรรมนูญ ดังนั้น The CAN-SPAM Act จึงถูกล้อมรอบด้วยการวิพากษ์อย่างหนักหน่วงว่าอ่อนเกินไป และแข็งเกินไป จากกลุ่มที่ตรงกันข้ามทั้งสองฝ่ายด้วยความคาดหวังที่แตกต่างกัน ซึ่งเป็นสิ่งที่บ่งบอกถึงความไม่กลมกลืนกันอันเป็นผลลัพธ์ในการถกเถียงกันโดยทั่วๆ ไปในการจัดการกับอินเตอร์เนต และชี้ให้เห็นถึงการขาดการยอมรับอย่างเป็นเอกฉันท์ซึ่งความคิดที่จะบรรลุจุดมุ่งหมายได้ดีที่สุดในการต่อสู้กับสแปม

3.4.4.1 การให้คำจำกัดความของคำว่า "สแปมเมล"

ประเด็นแรกที่เป็นข้อถกเถียงในกฎหมายฉบับนี้[19] ก็คือเรื่อง คำนิยามของคำว่า "สแปมเมล" ในการบัญญัติกฎหมาย หรือการให้คำนิยามของคำว่าสแปมเมล อย่างเป็นทางการ มักจะมีผู้ให้ความหมายเอาไว้หลายประการ แต่คำที่ใช้เรียกสแปมเมลและนำมาใช้อ้างอิงอยู่บ่อยครั้งในภาษาอังกฤษ ก็คือคำว่า unsolicited commercial e-mail (UCE) และ unsolicited bulk e-mail (UBE) ความแตกต่างระหว่างความหมายของทั้งสองคำนี้น่าจะเป็นเรื่องทางทฤษฎีมากกว่า โดยปรากฏว่าน่าจะมีความเกี่ยวพันกับปริมาณของจำนวนสแปมเมลที่ถูกส่งในแต่ละครั้งการใช้คำว่า UBE จะเน้นถึงปริมาณมหาศาลของสแปมแมล์ที่ถูกส่งออกไป โดยมีค่าใช้จ่ายที่ต่ำเพียงไม่กี่ดอลล่าห์ อีเมลจำนวนหลายล้านฉบับก็จะถูกส่งออกไป ซึ่งไม่มีวิธีการอื่นใด ที่สามารถทำได้เช่นนั้น และด้วยต้นทุนที่ต่ำเช่นนี้จึงเป็นที่ดึงดูดสแปมเมอร์ทั้งหลายให้ใช้วิธีการดังกล่าว ในขณะที่บริษัทที่มีชื่อเสียงส่วนใหญ่จะไม่ทำเช่นนั้น เนื่องจากอัตราการตอบสนองที่ต่ำ และคาดหวังความโกรธเคืองมากกว่าได้ลูกค้า

โดยกฎหมายฉบับนี้ คำว่า "สแปมเมล" นั้นไม่ได้มีการนิยาม หรืออ้างถึงโดยเฉพาะ แม้จะปรากฏคำว่า "CAN-SPAM" แต่ก็เป็นเพียงคำย่อของชื่อเต็มของกฎหมายนี้เท่านั้น และไม่ได้มีความหมายโดยนัยแต่อย่างใด แม้คำว่า สแปมเมล จะเป็นคำที่ใช้เรียกจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ร้องขอโดยทั่วไป แต่ในกฎหมายฉบับนี้กล่าวอ้างถึงอีเมลที่มีลักษณะดังกล่าวโดยใช้คำว่า UCE ซึ่งเป็นการนิยามโดยเน้นถึงเนื้อหาของอีเมลเท่านั้น โดยใน Section 3(2)(A) of the CAN-SPAM Act ได้ให้คำนิยามของคำว่า a commercial electronic message ว่าเป็น "ข้อความอีเมลใดๆ ที่มีวัตถุประสงค์เบื้องต้นซึ่งเป็นการโฆษณาเชิงพาณิชย์ หรือเป็นการส่งเสริมสินค้าหรือบริการเชิงพาณิชย์ (รวมถึงที่มีเนื้อหาของอินเตอร์เนตเวปไซต์ที่มีวัตถุประสงค์เกี่ยวข้องในเชิงพาณิชย์ด้วย)" โดยน่าจะ

---

[19] Taiwo A. Oriola, "Regulating Unsolicited Commercial Electronic Mail in the United States and the European Union: Challenges and Prospects," Tulane Journal of Technology & Intellectual Property 7,113 (spring 2005) : 2.

ครอบคลุมถึงรูปแบบของอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอทั้งหมด ทั้งอีเมลที่ส่งทาง SMTP-based แต่ดั้งเดิมและระบบการส่งข้อความอิเล็กทรอนิกส์อื่นๆ เช่น เอสเอ็มเอส และเอ็มเอ็มเอส

ทั้งนี้ หลายฝ่ายเห็นว่า สแปมเมลจำนวนมากที่สามารถส่งออกไปได้ในครั้งเดียวหรือที่เรียกว่า bulk email เป็นปัญหาสำคัญที่กระตุ้นการเติบโตของสแปมเมล การออกกฎหมายจึงควรคำนึงถึงผู้ส่งสแปมเมลประเภทนี้มากกว่า ซึ่งหากกฎหมายให้คำนิยามกฎเกณฑ์ในการส่งเมลโดยคำนึงถึงปริมาณ ก็จะสามารถลดจำนวนสแปมเมลลงได้มากกว่าการสร้างเงื่อนไขให้อนุญาตทำการพาณิชย์ได้โดยวิธีสแปมเมล นอกจากนี้ การมุ่งประเด็นไปที่อีเมลเชิงพาณิชย์ที่ไม่พึงประสงค์ อันเป็นการมุ่งไปที่เนื้อหาของอีเมล มากกว่าประเด็นเรื่องวิธีในการส่งอีเมล เป็นเรื่องที่อันตรายอย่างมากและอาจมีผลในเรื่องความชอบธรรมตามรัฐธรรมนูญ

นอกจากนั้น ยังมีข้อความอีเมลที่ไม่ใช่เพื่อการพาณิชย์อีกจำนวนหนึ่งที่เรียกว่า Fortiori เช่น สปีชทางการเมือง หรือจดหมายขอความรัก เป็นต้น ที่ไม่จัดว่าเป็นสแปมเมลตามกฎหมายฉบับนี้ แม้ว่าอีเมลเหล่านั้นจะได้รับความเห็นตรงกันว่าเป็นสแปมเมลก็ตาม แต่การห้ามการส่งสแปมเมลใดที่มีผลกระทบโดยตรงต่อการพูดในเชิงการเมือง หรือการส่งอีเมลที่ไม่ใช่เพื่อการพาณิชย์ ก็อาจถูกกล่าวอ้างถึงประเด็นเรื่องความชอบธรรมตามรัฐธรรมนูญได้

อย่างไรก็ตาม ความแตกต่างของ UBE และ UCE ส่งผลต่อการจัดการกับสแปมเมลเพียงเล็กน้อย เพราะสแปมส่วนใหญ่เกี่ยวพันในเชิงพาณิชย์อย่างเป็นปกติ ทำให้กฎหมายต่อต้านสแปมเมลในหลายประเทศ มุ่งจัดการกับอีเมลที่ไม่ได้ร้องขอในเชิงพาณิชย์เป็นประเด็นสำคัญ

3.4.4.2 ประสิทธิภาพในการบังคับใช้กฎหมาย

อุปสรรคสำคัญที่มีผลทำให้การบังคับใช้ CAN SPAM Act of 2003 ไม่มีประสิทธิภาพมากนักได้แก่

<u>ประเด็นที่หนึ่ง</u> ผลของกฎหมายฉบับนี้ ทำให้การส่งสแปมเมลกลายเป็นสิ่งที่ยอมรับได้ตามกฎหมาย ตราบใดที่การส่งสแปมเมลนั้น อยู่ภายในหลักการและขอบเขตของกฎหมาย เช่นการมีที่อยู่อีเมลที่แท้จริงของผู้ส่ง หรือการใช้ข้อความหัวข้ออีเมลที่เชื่อถือได้ นอกจากนี้ การพิสูจน์ตัวผู้กระทำผิดในทางอาญา เพื่อนำตัวมาขึ้นศาล ก็ยังเป็นเรื่องยาก เพราะสแปมเมอร์มีความเชี่ยวชาญในการปกปิดตัวตนที่แท้จริงของตนเอง เช่นการใช้อุปกรณ์ออนไลน์ของผู้อื่น หรือการลักลอบเข้าไปใช้เครื่องคอมพิวเตอร์ของผู้อื่นเพื่อทำการส่งสแปมเมลโดยที่ผู้เป็นเจ้าของไม่อาจทราบได้ หรือการส่งสแปมเมลจากประเทศอื่น ทำให้กฎหมายไม่สามารถใช้บังคับได้

ประเด็นที่สอง หากผู้รับยินยอมให้ข้อมูลแก่เจ้าของเวปไซต์ หรือผู้ให้บริการอีเมลที่ทำให้ผู้บริการสามารถเก็บรวบรวมข้อมูลส่วนตัวดังกล่าวไปใช้ โดยที่ผู้รับไม่อาจทราบถึงข้อจำกัดที่ชัดเจนในการใช้ข้อมูลจากผู้ให้บริการได้ ผู้ใช้จึงไม่อาจทราบได้ว่าอีเมลที่ถูกเก็บรวบรวมไปนั้น ถูกนำไปใช้ด้วยความซื่อสัตย์เพียงใด เพราะการส่งอีเมลเชิงพาณิชย์ และการส่งสแปมนั้นมีความใกล้เคียงกัน จนไม่สามารถแยกออกจากกันได้อย่างชัดเจน ผลของกฎหมายฉบับนี้ จึงเสมือนเป็นการยอมให้ผู้เก็บรวบรวมสามารถนำข้อมูลที่มีไปแสวงหาผลประโยชน์ส่วนตัวได้นับครั้งไม่ถ้วน หากว่าได้ระบุข้อความอนุญาตให้ใช้ข้อมูลลงบนเวปไซท์ ซึ่งผู้บริโภคอาจมิได้สังเกตเห็นได้

ประเด็นที่สาม ความแตกต่างทางด้านมาตรการที่นำมาใช้ ระหว่างวิธีการ "Opt-in"* ซึ่งต้องการให้ผู้รับให้ความยินยอมอย่างชัดแจ้งก่อน ในการบอกรับอีเมลเชิงพาณิชย์ที่อาจถูกส่งมาในภายหลัง อันเป็นสิ่งจำเป็นต่อการลดปริมาณการเพิ่มขึ้นของสแปมเมลอย่างมาก ในขณะที่ "Opt-out"♣ เป็นการสนับสนุนการเพิ่มขึ้นของการทำการตลาดโดยวิธีการส่งสแปมเมล นอกจากนั้น วิธีการ "Opt-out" ยังก่อให้เกิดภาระแก่ผู้บริโภคที่ไม่ต้องการรับอีเมลเชิงพาณิชย์ ในการบอกยกเลิกการรับอีเมลจากผู้ส่ง และขอให้ผู้ส่งลบรายชื่ออีเมลของตนออกจากรายชื่อกลุ่มเป้าหมาย ซึ่งขั้นตอนดังกล่าวมีความยุ่งยากแตกต่างกันมากมาย และก่อให้เกิดภาระแก่ผู้รับโดยปริยายหากไม่ต้องการอีเมลเหล่านี้ อีกทั้ง ผู้รับส่วนใหญ่มักไม่ต้องการที่จะติดต่อใดๆ กับผู้ส่งสแปมเมล จึงทำให้มีผู้รับเพียงเล็กน้อยเท่านั้น ที่ยอมสละเวลาของตนเองในการปฏิบัติตามขั้นตอนเหล่านั้น

ผลกระทบโดยอ้อมที่ได้รับจากการกำหนดให้ใช้วิธี "Opt-out" ตามกฎหมายทำให้บริษัทที่ทำการตลาดออนไลน์ส่วนใหญ่ ที่ใช้วิธีทำการตลาดบนพื้นฐานของการขออนุญาตจากผู้รับ หรือการใช้รูปแบบธุรกิจแบบ "Opt-in" อยู่แล้ว สนใจการทำการตลาดโดยรูปแบบทางกฎหมายแบบ "Opt-out" มากขึ้น นอกจากจะเป็นการลดจำนวนธุรกิจที่ปฏิบัติต่อผู้บริโภคโดยยึดถือความสมัครใจของผู้บริโภคเป็นหลักแล้ว ยังเป็นการให้การปกป้องทางกฎหมายแก่ผู้ที่ไม่ได้ทำการตลาดโดยวิธี "Opt-in" อีกด้วย นอกจากนั้น การใช้รูปแบบทางกฎหมายแบบ "Opt-out" ผู้ส่งต้องมีความซื่อสัตย์พอสมควร อันเป็นการยากสำหรับรัฐในการควบคุม เพราะการที่ผู้ส่งบอกยกเลิกการรับอีเมล ถือเป็นการยอมรับโดยอ้อมว่า ผู้รับนั้นมีตัวตนอยู่จริง และใช้อีเมลนั้นเป็นปกติวิสัย อันจะทำให้อีเมลนั้นมีมูลค่ามากขึ้นในการนำไปใช้ต่อไป

---

* วิธีการ "Opt-in" คือการให้ผู้บริโภคแสดงความสมัครใจในการรับอีเมลเชิงพาณิชย์ที่อาจถูกส่งไปจากผู้ประกอบการในภายหน้า โดยอาจเป็นการให้ความยินยอมโดยตรง หรือโดยอ้อมก็ได้

♣ วิธีการ "Opt-out" คือการให้ผู้บริโภคสามารถบอกเลิกการรับอีเมลเชิงพาณิชย์จากผู้ประกอบการที่ต้องการส่งมาในอนาคต โดยอาจมีขั้นตอนและวิธีการต่างๆ เพื่อให้ผู้ส่งสามารถทราบได้ว่าผู้รับไม่ต้องการรับอีเมลเช่นนั้นอีกต่อไป

<u>ประเด็นที่สี่</u> การบังคับใช้กฎหมายฉบับนี้ โดยกฎหมายฉบับนี้ผู้ที่ได้รับความเสียหายจากการได้รับสแปมเมล สามารถเยียวยาความเสียหายได้ โดยการดำเนินคดีแก่ผู้ส่งสแปมเมล ซึ่งบุคคลเหล่านั้น ได้แก่ เจ้าหน้าที่ของรัฐบาลกลาง อัยการรัฐ และผู้ให้บริการอินเตอร์เนต แต่การบังคับใช้กฎหมายโดยเจ้าหน้าที่รัฐบาลกลางและอัยการรัฐ อาจไม่ประสบผลสำเร็จเท่าที่ควร เนื่องจากไม่มีแหล่งข้อมูลที่จำเป็นต่อการบังคับใช้กฎหมายต่อต้านสแปม และต้องอาศัยความร่วมมือระหว่างรัฐอย่างสูง โดยในการนี้ รัฐจำต้องอาศัยเงินทุนจำนวนมาก เพื่อให้เจ้าหน้าที่สามารถบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพ มิฉะนั้น รัฐต้องยอมให้อำนาจแก่ผู้บริโภคในการฟ้องคดีเพื่อเยียวยาความเสียหายของตนเอง ซึ่งยังไม่สามารถกระทำได้

3.4.4.3 The Can-Spam Act: กับบริบทที่มีต่อกฎหมายรัฐธรรมนูญของสหรัฐฯ[20]

เนื่องจากกฎหมายรัฐธรรมนูญถือเป็นบทบัญญัติสูงสุด อันบัญญัติรับรองถึงสิทธิอันพึงมีขั้นพื้นฐานของประชาชนชาวสหรัฐฯ ดังนั้น กฎหมายทุกฉบับจึงต้องอยู่ภายใต้ขอบอำนาจของรัฐธรรมนูญเป็นสำคัญ

A. เสรีภาพเชิงพาณิชย์ กับกฎหมายสแปมของรัฐ (The Dormant Commerce Clause and State Spam Laws)

"Commerce Clause" เป็นบทบัญญัติในกฎหมายรัฐธรรมนูญของสหรัฐฯ ที่ให้อำนาจแก่สภาคองเกรซเท่านั้นในการออกกฎเกณฑ์ทางการค้าระหว่างชาติอื่นๆ และระหว่างรัฐด้วยกันเอง โดยผลของกฎหมายรัฐธรรมนูญ มลรัฐแต่ละรัฐยังคงสามารถบังคับใช้กฎหมายต่อต้านสแปมเมลของตนเองได้ เนื่องจาก CAN-SPAM Act ไม่ได้มีอำนาจเหนือกฎหมายสแปมของมลรัฐโดยสมบูรณ์ โดย CAN-SPAM Act จะไม่บังคับใช้ก่อนกฎหมายสแปมของมลรัฐที่ห้ามการปลอมแปลงและการหลอกลวงข้อความอีเมลเชิงพาณิชย์ อย่างไรก็ตาม อำนาจของอัยการรัฐที่จะฟ้องจำเลยที่ส่งข้อความอีเมลที่ปลอมแปลงและหลอกลวงจะถูกระงับไปโดยอัตโนมัติ ถ้า FTC หรือตัวแทนของรัฐบาลกลางอื่นๆ ตกลงที่จะฟ้องเป็นคดีในฐานะพลเมืองต่อจำเลยภายใต้เงื่อนไขที่เกี่ยวข้องใน CAN-SPAM Act.

---

[20] Ibid., p. 10.

เนื่องจากข้อความอีเมลเชิงพาณิชย์นั้นมีความเกี่ยวข้องในทางการค้า ดังนั้นจึงไม่อาจหลีกเลี่ยงที่จะกล่าวถึงประเด็นความสมบูรณ์ของกฎหมายสแปมของมลรัฐในบริบทเรื่องเสรีภาพในการพาณิชย์ ภายใต้รัฐธรรมนูญของสหรัฐ ( the Commerce Clause of the United States Constitution) โดยใน Article 1, Section 8, Clause 3 ของรัฐธรรมนูญได้ให้อำนาจสภาคองเกรส "ที่จะออกกฎหมายด้านการค้ากับชาติต่างประเทศ และระหว่างรัฐด้วยกัน และกับชนเผ่าอินเดียน"[21] ในคดี Healy v. The Beer Institute[22] ศาลสูงได้กล่าวว่า "การให้อำนาจกับสภาคองเกรซในเรื่องนี้ ยังแฝงไว้ด้วยการจำกัดอำนาจของรัฐโดยปริยายที่จะตรากฎหมายที่มีผลต่อการค้าระหว่างรัฐด้วย The Commerce Clause จึงเป็นพื้นฐานของหลักกฎหมายอันยาวนานว่า ห้ามรัฐในการออกกฎในทางที่เป็นอันตรายต่อการค้าระหว่างรัฐ แม้ว่าในขณะนั้นจะไม่มีกฎหมายที่ออกโดยสภาคองเกรซก็ตาม และยังถูกนำมาประยุกต์ใช้กับกฎหมายที่เกี่ยวกับการค้าจำนวนมากโดยศาลสูง ด้วยผลลัพธ์ที่แตกต่างกัน (ส่วนมากขึ้นอยู่กับข้อเท็จจริงโดยเฉพาะของแต่ละคดี) ซึ่งอาจห้ามการออกกฎหมายโดยมลรัฐในประเด็นที่ว่าไม่ชอบด้วยรัฐธรรมนูญ หรือฝ่าฝืนต่อ Commerce Clause

สภานิติบัญญัติได้อ้างถึง the dormant Commerce Clause เพื่อต่อต้านการออกกฎหมายเรื่องภาพลามกและสแปมบนอินเตอร์เนตของรัฐ คดี Ferguson v. Friendfinders Inc[23] เป็นตัวอย่างในเรื่องนี้ โดย Mark Ferguson โจทก์ซึ่งเป็นผู้รับอีเมลฟ้องคดีนี้ในปี 1999 กล่าวหาว่า Friendfinders และบริษัทอื่น ส่งอีเมลที่ไม่ได้ร้องขอที่ก่อให้เกิดความเข้าใจผิดและหลอกลวงถึงเขา และไม่ได้ปฏิบัติตามกฎหมายต่อต้านสแปมของแคลิฟอร์เนียด้วย ภายใต้กฎหมายแคลิฟอร์เนียซึ่งไม่ได้ออกกฎเรื่องอินเตอร์เนต หรือการใช้อินเตอร์เนตโดยตรง แต่ออกกฎต่อปัจเจกชนหรือนิติบุคคลที่ (1) ทำธุรกิจในแคลิฟอร์เนีย (2) ใช้ประโยชน์จากเครื่องมือที่ตั้งอยู่ในแคลิฟอร์เนีย และ (3) ส่ง UCE ถึงผู้อาศัยในแคลิฟอร์เนีย โดยสแปมทั้งหมดที่ส่งโดยชาวแคลิฟอร์เนีย หรือบุคคลใดๆ ถึงผู้รับในรัฐเดียวกันต้องมีเงื่อนไขการบอกเลิก หรือจ่าหน้า (ที่บอกว่าเป็นข้อความโฆษณา) ในบรรทัดหัวข้อ จำเลยท้าทายต่อคดีโดยกล่าวอ้างว่ากฎหมายฉบับนี้ละเมิด the dormant Commerce Clause ของรัฐธรรมนูญสหรัฐอเมริกา ศาลพบว่ามาตรา 17538.4 ของ California Business and Professions Code ไม่ได้แบ่งแยก หรือออกกฎโดยตรง หรือควบคุมการค้าระหว่างรัฐ ดังนั้น มาตรานี้จึงไม่ได้

---

[21] U.S. Const. art. 1, 8, cl. 3.

[22] 491 U.S. 324, 326 n.1 (1989).

[23] Reagan Smith, "Eliminating The Spam From Your Internet : the possible effects of the unsolicited commercial electronic mail act of 2001 on junk e-mail," Texas Tech Law Review 35, 411 (2004) : 10.

ละเมิด Commerce Clause เพราะว่าได้รับใช้ผลประโยชน์สาธารณะท้องถิ่นอย่างถูกกฎหมาย ในการปฏิเสธข้ออ้างของจำเลยว่ากฎหมายแคลิฟอร์เนียได้ขยายขอบเขตกฎหมายออกไปยังรัฐอื่นอย่างกว้างขวาม ศาลให้ความเห็นหนึ่งในหลายๆ ประเด็นว่า[24] "การขยายมาตรา 17538.4 ที่ต้องการความเป็นจริงในการโฆษณา ไม่เป็นภาระต่อการค้าระหว่างรัฐแต่อย่างใด แต่กลับเป็นการอำนวยความสะดวกต่อการค้าระหว่างรัฐโดยการกำจัดการฉ้อโกงและการหลอกลวงด้วย"

ศาลได้ให้ความเห็นที่แตกต่างกันในคดี American Libraries Ass'n v. Pataki[25] โดยโจทก์และนิติบุคคลอื่นๆ ที่ใช้อินเตอร์เนตเพื่อการสื่อสารได้ท้าทายความถูกต้องตามรัฐธรรมนูญของกฎหมายนิวยอร์กที่บัญญัติให้ การใช้คอมพิวเตอร์แพร่กระจายภาพลามกหรือวัตถุลามกไปยังผู้เยาว์เป็นความผิดอาญา โดยกล่าวหาว่าเป็นการละเมิด the First Amendment และ the Commerce Clause ตามรัฐธรรมนูญ จึงมีการฟ้องคดีเพื่อขอให้มีการเยียวยาเบื้องต้นก่อน โดยการห้ามเจ้าหน้าที่หรืออัยการของนิวยอร์คจากการบังคับใช้กฎหมายนี้

ทั้งนี้ ผลของการพิจารณาของศาลเขตสหรัฐฯ นั้นเห็นว่าคำตัดสินในคดี American Libraries ของศาลเขตใต้ของนิวยอร์ก ในเรื่องกฎหมายเกี่ยวกับภาพลามกทางอินเตอร์เนตของรัฐนิวยอร์กนั้นเหมาะสมแล้ว เนื่องจากนัยสำคัญของกฎหมายและบทบัญญัติที่ได้เปรียบรัฐอื่นในการจัดการกับสแปมบนไซเบอร์สเปซในการสื่อสารระหว่างรัฐ โดยผู้พิพากษาศาลเขตให้ความเห็นว่ากฎหมายประยุกต์ใช้กับการสื่อสารภายในรัฐ และระหว่างรัฐอย่างเห็นได้ชัด และชนิดของการสื่อสารนั้นเกี่ยวข้องกับการค้าตามรัฐธรรมนูญ ซึ่งมีความเป็นไปได้ที่กฎหมายจะมีผลกระทบที่เข้าถึงรัฐอื่นๆ เนื่องจากลักษณะที่แพร่หลายซึ่งเป็นลักษณะเฉพาะของอินเตอร์เนต โดยศาลเห็นว่า ลักษณะเช่นนี้สามารถนำไปสู่การกระทำผิดทางอาญาในนิวยอร์ก ซึ่งอาจถูกกฎหมายในรัฐอื่น โดยศาลให้เหตุผลว่าเหตุการณ์เช่นนี้จะเป็นการทำให้นโยบายรัฐของผู้ใช้อินเตอร์เนตอื่น อยู่ในฐานะที่เป็นรอง ซึ่งบางทีรัฐนั้นอาจจะสนับสนุนเสรีภาพของการแสดงออกเหนือกว่าแนวทางการป้องกันดังเช่นที่ปรากฏในรัฐนิวยอร์คอย่างมาก รัฐนิวยอร์คได้บัญญัติกฎหมายเรื่องอินเตอร์เนตของตัวเองออกมาโดยความตั้งใจ และผลของการนั้นทำให้กฎหมายของตนเองเข้าไปยังรัฐอื่นๆ ที่พลเมืองใช้อินเตอร์เนต การรุกล้ำเข้าไปเช่นนี้อยู่นอกเหนือจากเขตอำนาจซึ่งรัฐธรรมนูญได้มอบให้ไว้แก่รัฐบาลกลางโดยเฉพาะ และอยู่เหนืออำนาจอธิปไตยของรัฐอื่นๆ จึงเป็นการละเมิดโดยตรงต่อบทบัญญัติรัฐธรรมนูญในเรื่องการค้าการพาณิชย์

---

[24] Taiwo A. Oriola, p.10.

[25] Ibid., p. 10.

แม้ว่าผลการพิจารณาคดีของศาลได้กล่าวถึงลักษณะที่แพร่หลายของอินเตอร์เนต แต่ก็ให้ผลลัพธ์ในทางตรงกันข้าม ซึ่งอาจไม่ชอบด้วยเหตุผลที่จะแยกแยะที่ตั้งทางกายภาพต่อการใช้อินเตอร์เนต เพราะในทุกกรณี ผู้ใช้อินเตอร์เนต ไม่อาจทราบได้และไม่ได้สนใจในเรื่องที่ตั้งทางกายภาพในแหล่งกำเนิดของอินเตอร์เนตที่พวกเขาเข้าไปใช้ เพราะถูกออกแบบมาให้ละเลยต่อที่ตั้งทางกายภาพตามเอกสารมากกว่า ขณะที่คอมพิวเตอร์บนเครือข่ายนั้นมี "ที่อยู่" ซึ่งเป็นที่อยู่ที่ใช้บนเครือข่ายมากกว่าที่อยู่ทางกายภาพในพื้นที่จริง ที่อยู่ทางอินเตอร์เนตส่วนมากนั้นไม่ได้บ่งบอกที่ตั้งใดทางภูมิศาสตร์ และแม้ว่าที่อยู่ทางอินเตอร์เนตบางครั้งจะสามารถทราบถึงที่ตั้งได้ แต่ก็อาจก่อให้เกิดความเข้าใจผิดได้ง่าย ยิ่งไปกว่านั้น ไม่มีลักษณะใดที่เป็นไปได้ของอินเตอร์เนตที่จะสามารถปิดกั้นผู้ใช้จากรัฐอื่น ผู้ใช้อินเตอร์เนตที่สร้างเวปเพจ ไม่สามารถป้องกันชาวนิวยอร์กเกอร์ หรือชาวโอกลาโฮมา หรือชาวไอโอว่า จากการเข้าถึงหน้าเวปเพจนั้นได้ และไม่มีทางที่จะรู้ได้ว่าผู้เยี่ยมชมจากรัฐใดที่เข้ามาเยี่ยมชมเวปไซต์นั้น อีกทั้งไม่มีผู้เข้าร่วมสนทนาในห้องสนทนาคนใดสามารถป้องกันผู้เข้าร่วมคนอื่นจากรัฐใดโดยเฉพาะในการเข้าร่วมสนทนา และผู้ส่งที่ใช้โปรแกรมกระจายเมล จะไม่อาจทราบได้ถึงอัตราการเพิ่มขึ้นหรือลดลงที่แท้จริงของบัญชีการส่งเมลว่า ได้จำกัดผู้ใช้จากรัฐใดแล้ว เพราะว่าผู้ใช้สามารถเพิ่มหรือถอนรายชื่อของตนออกจากบัญชีการส่งเมลได้โดยอัตโนมัติ ดังนั้น ผู้ที่เลือกบัญชีส่งอีเมลที่เชื่อว่าไม่ได้รวมชาวนิวยอร์กคนใดเอาไว้ แต่ชาวนิวยอร์กที่ถูกเพิ่มหลังจากนั้นก็ยังอาจจะได้รับข้อความเหล่านั้นได้

คดี American Libraries จึงเป็นชัยชนะที่มีนัยสำคัญต่อผู้สนับสนุนเงื่อนไขเรื่องเสรีภาพตาม First Amendment และเสรีภาพในการพูดอย่างอิสระ โดยเน้นให้เห็นถึงผลของการใช้สิทธิเกินเขตอำนาจโดยจงใจว่าเป็นอุปสรรคที่สำคัญต่อความสำเร็จของกฎหมายสแปมของรัฐที่มีความแตกต่างกัน อันแสดงให้เห็นถึงประโยชน์ของกฎหมายสแปมจากรัฐบาลกลาง

คดีที่กระทบถึงบทบัญญัติตามรัฐธรรมนูญเรื่องการค้าระหว่างรัฐ (Commerce Clause) จะมีผลลัพธ์ที่หลากหลาย ซึ่งในอดีตศาลสูงสหรัฐฯ อาจจะไม่เห็นด้วยหรือสนับสนุนความถูกต้องตามรัฐธรรมนูญของกฎหมายเช่นนั้น โดยคำตัดสินที่ขึ้นอยู่กับลักษณะเฉพาะของกฎหมายรัฐในประเด็นดังกล่าว กล่าวคือ ในทางประวัติศาสตร์แล้ว กฎหมายของรัฐจะตกไปหรือมีผลใช้บังคับนั้น ขึ้นอยู่กับพื้นฐานความเข้าใจของศาลสูงต่อผลกระทบที่เกิดขึ้นจากการใช้อำนาจเกินขอบเขตของกฎหมายฉบับนั้นที่มีต่อการค้าของรัฐอื่น ดังนั้น กฎหมายสแปมของมลรัฐอันแตกต่างกันในเนื้อหาโดยเฉพาะ จึงไม่สามารถหลีกเลี่ยงการตีความของศาลที่อาจจะก่อให้เกิดคำวินิจฉัยที่แตกต่างกันได้โดยศาลของรัฐกับสิทธิตาม Commerce Clause ซึ่งเป็นการลดประสิทธิภาพอันเป็นหลักสำคัญ

ในการควบคุมสแปม ซึ่งเป็นจุดหนึ่งที่เน้นให้เห็นถึงการความจำเป็นของการใช้บังคับ CAN-SPAM Act เหนือกฎหมายสแปมของรัฐ ดังเช่นที่ปรากฏในคดี State v. Heckel[26]

ในคดีนี้ Jason Heckel ได้ส่งสแปมเมลไปทั่วอินเตอร์เนตเพื่อทำการตลาดหนังสือเล่มหนึ่งที่เขาผลิตชื่อว่า "How to Profit From Internet" โดยได้ส่งอีเมลสแปมจำนวน 100,000 ถึง 1,000,000 ฉบับต่อสัปดาห์ ซึ่งถูกรายงานไปยังเจ้าหน้าที่คุ้มครองผู้บริโภคหลายครั้ง เจ้าหน้าที่ได้ส่งจดหมายถึง Heckel เพื่ออธิบายถึงกฎหมายต่อต้านการสแปมในรัฐวอชิงตัน และได้พูดคุยทางโทรศัพท์เพื่อขอให้เขาเลิกส่งสแปมเมล แต่ก็ไม่เกิดผลแต่อย่างใด

ดังนั้น ในเดือนตุลาคม ปี 1998 รัฐจึงฟ้องคดี Heckel โดยอ้างการกระทำสามข้อในการดำเนินธุรกิจที่เกี่ยวข้องกับสแปมของเขา Heckel แย้งว่า เป็นที่น่าสงสัยว่ากฎหมายวอชิงตันละเมิด Dormant Commerce Clause เพราะว่ารัฐออกกฎหมายถึงการกระทำต่อผู้รับสแปมในรัฐอื่น ซึ่งในที่สุดศาลก็ได้ปฏิเสธข้อโต้แย้งอันนี้

ในการอุทธรณ์ ศาลชี้ว่ากฎหมายต่อต้านสแปมเมลของรัฐวอชิงตันไม่ได้ละเมิดบทบัญญัติเรื่องการค้าภายในตามรัฐธรรมนูญ ตามความเห็นของศาลสูงวอชิงตัน เห็นว่ากฎหมายได้จำกัดสแปมอันเป็นภัยต่อประชาชนและธุรกิจในรัฐ ดังนั้นผลประโยชน์ของรัฐตามกฎหมายฉบับนี้จึงมีน้ำหนักกว่าภาระใดที่บัญญัติขึ้นเพื่อการส่งสแปม โดยศาลให้เหตุผลว่า ภาระอย่างเดียวที่กฎหมายต่อต้านสแปมก่อขึ้นต่อสแปมเมอร์คือ การเปิดเผยตัวตนที่แท้จริงของผู้ส่งสแปม อันเป็นความต้องการที่ไม่เป็นภาระต่อการพาณิชย์แต่อย่างใด ในทางตรงกันข้ามกลับเอื้อประโยชน์ต่อพาณิชย์ในการกำจัดการฉ้อโกงและหลอกลวงด้วย

แม้ว่าศาลสูงวอชิงตัน จะอ้างเขตอำนาจศาลของบุคคลเหนือสแปมเมอร์จากรัฐโอเรกอน และแสดงว่ากฎหมายคุ้มครองผู้บริโภคของรัฐวอชิงตันนั้นชอบด้วยรัฐธรรมนูญในเรื่องที่เกี่ยวกับ Commerce Clause แต่ไม่เป็นการยืนยันว่าศาลสูงสหรัฐฯ จะให้ความเห็นอย่างเดียวกันในการตีความความถูกต้องตามรัฐธรรมนูญของกฎหมายคุ้มครองผู้บริโภคของรัฐวอชิงตันในบริบทของ Commerce Clause ยิ่งไปกว่านั้น คำวินิจฉัยของศาลสูงวอชิงตันยังเป็นคำวินิจฉัยในเรื่องความถูกต้องตามรัฐธรรมนูญของกฎหมายของรัฐวอชิงตันเองด้วย ดังนั้น คดีนี้จึงมีความเป็นไปได้ว่าศาลสูงสหรัฐฯ จะยึดถือ Commerce Clause มากกว่ากฎหมายสแปมของรัฐ ที่ปรากฏหลักฐานของการให้ความคุ้มครองเพียงเล็กน้อย แต่มีผลกระทบจากการใช้อำนาจนอกอาณาเขต ที่ปรากฏว่าก้าวก่าย

---

[26] Reagan Smith, "Eliminating The Spam From Your Internet : the possible effects of the unsolicited commercial electronic mail act of 2001 on junk e-mail," Texas Tech Law Review 35, 411 (2004) : 11.

หรือเป็นอุปสรรคต่อการค้าระหว่างรัฐ โดยเฉพาะรัฐบาลกลาง ที่ต้องการประสานผลประโยชน์ที่หลากหลายของรัฐต่างๆ ให้เกิดความสมดุลกัน แม้ว่ามลรัฐที่บัญญัติกฎหมายเช่นนั้นจะได้รับแรงจูงใจเป็นพิเศษจากผลประโยชน์สาธารณะท้องถิ่นอย่างถูกกฎหมายก็ตาม ดังนั้น ลักษณะสำคัญอีกประการหนึ่งของกฎหมายสแปมของรัฐที่เห็นได้ชัดของ The CAN-SPAM Act คือสามารถหลีกเลี่ยงการปะทะกันที่อาจเป็นไปได้อย่างมีประสิทธิภาพ ระหว่างกฎหมายสแปมของรัฐที่แตกต่างกันและ Commerce Clause ทำให้กฎหมายหลุดพ้นจากทางตันทางรัฐธรรมนูญที่เกิดจาก Commerce Clause ต่อกฎหมายสแปมของรัฐ ความเป็นหนึ่งเดียวกันของ CAN-SPAM Act ซึ่งตรงกันข้ามกับกฎหมายสแปมของรัฐ จึงเป็นผลให้เกิดการเผชิญหน้าที่ดีกว่าในการต่อสู้กับสแปม เมื่อเทียบกับวิธีอื่น

B. Advertisement Labeling and the First Amendment

มาตรา 5(a)(5)(A)(i) ของ CAN-SPAM Act ถือว่าเป็นการกระทำที่ผิดกฎหมายในการส่งข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ไปยังคอมพิวเตอร์ที่ได้รับการปกป้อง โดยปราศจาก "ลักษณะบ่งชี้ที่ชัดเจนและเห็นได้โดยชัดแจ้งว่าข้อความนั้นเป็นการโฆษณา หรือการชักชวน" เช่นเดียวกันกับมาตรา 5(d)(1) ที่กำหนดให้แสดงข้อความเหมือนเป็นฉลากเตือนว่าเป็นอีเมลที่ไม่ได้ร้องขอที่แนะนำเกี่ยวกับเรื่องเพศ เงื่อนไขการให้มีฉลากนี้ให้อำนาจอย่างเห็นได้ชัดแก่ ISP และผู้บริโภคที่แยกแยะได้อย่างง่ายๆ และกลั่นกรองข้อความอิเล็กทรอนิกส์ที่ถูกแนะนำว่าเกี่ยวกับเพศ หรือเชิงพาณิชย์ที่ไม่ได้ร้องขอได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม ปัญหาหลักๆ สองประการที่เกิดจากเงื่อนไขการมีฉลากคือ ประเด็นแรก เงื่อนไขการมีฉลากไม่ได้ใช้บังคับเพื่อต่อต้านอีเมลที่แพร่กระจายมาจากภายนอกสหรัฐฯ และประการที่สอง เงื่อนไขนี้ไม่ได้กำหนดมากไปกว่าการก่อตั้ง "forced speech" *และดังนั้นจึงเป็นการฝ่าฝืนต่อ First Amendment ประเด็นเหล่านี้เป็นปัญหาที่น่าวิตกที่ตระหนักได้ถึงวัตถุประสงค์ในการมีฉลากโฆษณาของ the CAN-SPAM Act ปัญหาทั้งสองประการกับแนวทางของศาลสหรัฐฯ กับวิธีการจัดการปัญหา วิเคราะห์ได้ดังนี้

(1) การบังคับใช้ตามเงื่อนไขการมีฉลากกับผู้ส่งข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอจากภายนอกสหรัฐฯ

---

* "forced speech" คือถูกจำกัดสิทธิ เสรีภาพในการแสดงความคิดเห็น อันถือเป็นการไม่ชอบด้วยบทบัญญัติตามรัฐธรรมนูญของสหรัฐฯ

ปัญหากฎหมายประเด็นแรกนี้ เกี่ยวข้องกับการบังคับใช้กฎหมายสแปมของชาติในทางระหว่างประเทศ สภาคองเกรซได้ตระหนักถึงปัญหานี้ในฐานะที่เป็นอุปสรรคสำคัญที่เป็นไปได้ และมันก็ไม่ใช่ปัญหาใหม่เสียทีเดียวนัก ในส่วนนี้จะตรวจสอบและชี้ให้เห็นถึงความคล้ายคลึงกัน โดยการเทียบเคียงกับของข้อขัดแย้งเกี่ยวกับเขตอำนาจศาลในไซเบอร์สเปซระหว่างประเทศในช่วงเวลาที่ผ่านมา และบทเรียนอะไรที่จะได้รับจากการบังคับใช้กฎหมายสแปมระหว่างประเทศ

Christopher Reed[27] ซึ่งเป็นผู้สนับสนุนให้มีการปฏิรูปกฎหมายแต่ดั้งเดิมบนไซเบอร์สเปซ โดยแนะนำให้ประยุกต์ใช้หลักการจำกัดถิ่นที่อยู่ (localization principle) ในการแก้ไขปัญหาเกี่ยวกับเขตอำนาจศาลในไซเบอร์สเปซ ซึ่งเกี่ยวข้องกับการสืบรู้ให้แน่ว่าบุคคลนั้นอยู่ที่ใดเมื่อการกระทำที่เกี่ยวข้องเกิดขึ้น ดังนั้น ศาลที่ตั้งอยู่ที่ๆ ข้อมูลดิจิตอลถูกอัพโหลดหรือดาวน์โหลด จึงสามารถคาดเดาได้ถึงเขตอำนาจศาล หรือประยุกต์กฎของศาลเหนือข้อขัดแย้งนั้นได้ หลักการนี้เน้นถึงตรรกะที่ซ่อนอยู่ในคดี Gutnick v. Dow Jones & Co.,[28] ของชาวออสเตรเลีย ที่ศาลสูงของวิคตอเรียอ้างถึงเขตอำนาจศาลเหนือบริษัทของสหรัฐฯ ในคดีฟ้องหมิ่นประมาทโดยพลเมืองชาววิคตอเรีย โดยที่ข้อความหมิ่นประมาทที่ถูกกล่าวหาถูกอัพโหลดบน www โดยจำเลยที่อยู่อาศัยในนิวยอร์ค ในชั้นอุทธรณ์ คำตัดสินของศาลซูพรีมวิคตอเรียถูกยืนตามอีกหนึ่งปีต่อมาโดยศาลฎีกาของออสเตรเลีย

ในคดี Dow Jones & Co. v. Gutnick ในคดีเทียบเคียงกันของ Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc., ผู้พิพากษาศาลเขตมีคำสั่งต่อจำเลยเรื่องการยอมรับค่าสมาชิกเพิ่มเติมจากลูกค้าในสหรัฐฯ สำหรับการเป็นสมาชิกนิตยสาร PLAYMEN ของชาวอิตาเลียน ซึ่งถูกตีพิมพ์บน www ในอิตาลี ศาลพบว่าการทำนิตยสารให้หาได้ง่ายต่อสมาชิกในสหรัฐฯ เป็นการละเมิดคำสั่งเยียวยาเมื่อวันที่ 26 มิถุนายน 1981 ของสหรัฐที่ยังมีอยู่ ซึ่งสั่งให้การใช้ PLAYMEN เป็นเครื่องหมายของตนในสหรัฐฯ เป็นการละเมิดเครื่องหมายการค้าของ Playboy

หลักการที่ซ่อนอยู่ในคดี Gutnick และ Playboy สามารถนำมาประยุกต์ใช้ได้โดยประมาณในการบังคับใช้เรื่องความต้องการให้มีฉลากโดยเฉพาะ และบังคับใช้กับเงื่อนไขอื่นๆ ของ CAN-SPAM Act โดยทั่วไป สำหรับสแปมที่กำเนิดจากภายนอกสหรัฐฯ อย่างไรก็ตาม ควรจะทราบว่าการประยุกต์ใช้กฎของท้องถิ่น และการถือเอาเขตอำนาจศาลโดยศาลท้องถิ่นเหนือข้อขัดแย้งระหว่าง

---

[27] Ibid., p. 12.

[28] Ibid., p. 12.

ประเทศผ่านหลักการจำกัดถิ่นที่อยู่นั้นก็มิใช่ว่าจะเป็นเรื่องที่ปลอดจากความขัดแย้งของปัญหาทางกฎหมายเสียที่เดียวนัก เหล่านี้มีต้นกำเนิดหลักๆ จากความแตกต่างในเนื้อหาและกระบวนการทางกฎหมายในแต่ละประเทศ ตัวอย่างเช่น พฤติกรรมที่ผิดกฎหมายอาญาในประเทศ A อาจจะเป็นสิ่งที่ถูกต้องตามกฎหมายของประเทศ B และกฎหมายสแปมของชาติก็มีความแตกต่างกันด้วย โดยเฉพาะในด้านเนื้อหา ตัวอย่างเช่น กฎหมายสแปมของอังกฤษ ซึ่งมีลักษณะเดียวกับประเทศในยุโรปส่วนมากบังคับใช้หลักการส่งสแปมที่อยู่บนพื้นฐานความยินยอมแบบ "opt-in" ซึ่งตรงกันข้ามกับวิธีการ "opt-out" ของสหรัฐ ยิ่งไปกว่านั้น ขณะที่ E-Privacy Directive ของกลุ่มยุโรปให้อำนาจบุคคลทั่วไปที่ได้รับความเดือดร้อนจากสแปมเมล ฟ้องคดีแพ่งต่อสแปมเมอร์ที่ละเมิดเงื่อนไขที่ได้รับการสนับสนุนจากรัฐสมาชิก ในขณะที่ CAN-SPAM Act ไม่มีเงื่อนไขในลักษณะเดียวกันนี้ สิ่งเหล่านี้เป็นลางร้ายของคำวินิจฉัยในการพิจารณาคดีที่แตกต่างกันเรื่องการกระทำความผิด, ความรับผิด, ค่าเสียหาย ที่เป็นการกระตุ้นการชอปปิ้งคดีโดยคู่ความอย่างแน่นอนลักษณะกลืนไม่เข้าคายไม่ออกเช่นนี้พิสูจน์ได้อย่างดีเยี่ยมในคดี Gutnick ที่ ศาลซูพรีมวิคตอเรีย โดยกล่าวว่าโจทก์มีโอกาสที่จะประสบความสำเร็จได้ดีกว่าในการฟ้องคดีหมิ่นประมาทต่อจำเลยในออสเตรเลีย เมื่อเปรียบเทียบกับสหรัฐฯ ที่ข้อเรียกร้องของเขาอาจจะไม่สามารถต้านทานต่อการพิจารณาตาม First Amendment. ได้

ยิ่งไปกว่านั้น หัวใจสำคัญต่อความสำเร็จของหลักการจำกัดถิ่นที่อยู่คือการยอมรับและการบังคับใช้คำตัดสินของต่างชาติที่เกี่ยวข้องกับสแปม ในกลุ่มสหภาพยุโรป ตาม Brussels Convention ยอมให้มีการยอมรับและบังคับใช้คำพิพากษาระหว่างรัฐสมาชิกโดยอิสระได้ อย่างไรก็ตาม ในสหรัฐฯ กระบวนการทางกฎหมายในการยอมรับและบังคับใช้คำพิพากษาระหว่างประเทศมีความแน่นอนน้อยมาก อุปสรรคสำคัญในการบังคับใช้คำพิพากษาของต่างชาติในสหรัฐฯ คือคำพิพากษาของต่างชาตินั้นไม่รวมอยู่ใน Full Faith and Credit Clause ตามรัฐธรรมนูญ ซึ่งต่างจากคำพิพากษาในระหว่างรัฐกันเอง ยิ่งไปกว่านั้น การยอมรับและบังคับใช้คำพิพากษาของต่างชาติอาจจะถูกปฏิเสธในระหว่างดำเนินการ ด้วยเหตุผลเรื่องเขตอำนาจศาลที่ไม่สมเหตุสมผลในการตัดสินคดี และกระบวนการพิจารณาที่บกพร่อง

ปัญหาอันยุ่งยากในเรื่องการยอมรับและบังคับใช้คำพิพากษาของต่างชาติในสหรัฐฯ มีแนวทางแห่งความยุ่งยาก โดยคำพิพากษาของฝรั่งเศสใน คดี Yahoo! เนื่องด้วยมีนัยที่สำคัญเรื่องการบังคับใช้คำพิพากษาของต่างชาติในการบังคับใช้กฎหมายสแปมระหว่างประเทศ โดยมีรายละเอียดของคดีคือ ศาลฝรั่งเศสพบว่า Yahoo! ต้องรับผิดในการละเมิดมาตรา R645-1 ของประมวลกฎหมายอาญาของฝรั่งเศส ซึ่งห้ามการจัดแสดงสินค้าเพื่อโฆษณา และงานฝีมือของ NAZI อันเป็นคดีระหว่าง Ligue

Contre le Racisme et L'Antisemitisme v. Yahoo! Inc[29] อย่างไรก็ตาม ศาลเขตสหรัฐฯ ทางตอนเหนือของแคลิฟอร์เนียในคดี Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisemitisme บนข้อเท็จจริงเดียวกัน ถือว่าคำสั่งของศาลฝรั่งเศสเป็นการละเมิดซึ่งอิสรภาพในการแสดงออกภายใต้บทบัญญัติของ First Amendment ตามรัฐธรรมนูญ คำตัดสินของศาลเขตเป็นข้อสมมติฐานว่า ถ้าคู่ความฝ่ายใดมีถิ่นที่อยู่ในฝรั่งเศสจะผูกมัดในการแสดงออกว่าผิดกฎหมายในฝรั่งเศส แต่ถูกกฎหมายในสหรัฐฯ และไม่น่าจะเป็นไปได้ที่ศาลสหรัฐฯ น่าจะหรืออาจจะใต่สวนการปรับใช้กฎหมายฝรั่งเศสต่อการกระทำของคู่สัญญานั้น อย่างไรก็ตาม คดีที่แตกต่างกันอย่างสิ้นเชิงอาจจะเกิดขึ้น ถ้าศาลฝรั่งเศสสั่งคู่ความไม่ให้ผูกมัดต่อการแสดงออกอย่างเดียวกันกับสหรัฐฯ บนหลักเกณฑ์ว่าพลเมืองฝรั่งเศส (เช่นเดียวกับคนอื่นๆ บนโลกที่มีวิธีที่จะทำเช่นนั้น) อาจจะอ่าน ได้ยิน หรือ เห็นมันในภายหลังได้ ขณะที่ การเข้าถึงอินเตอร์เนตอย่างมีประสิทธิภาพได้กำจัดหลักเกณฑ์ทางโลกและที่ตั้งทางกายภาพตามสมมติฐานนี้ออกไป ซึ่งการวิเคราะห์ทางกฎหมายก็จะเป็นเช่นเดียวกัน

อย่างไรก็ตาม ศาลอุทธรณ์ของสหรัฐฯ ได้กลับคำพิพากษาของศาลเขตในคดี Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisemitisme โดยศาลอุทธรณ์พบว่าศาลเขตถือเอาเรื่องเขตอำนาจศาลเหนือบุคคลอย่างไม่ถูกต้อง กว่าจะมีการตัดสินคดี ศาลอุทธรณ์ต้องไล่เลียงเอาความจริงอย่างหนักบนเงื่อนไขสามประการเรื่อง "minimum contacts" "fairplay" และ "substantial justice" ที่ศาลซูพรีมยึดถือเหมือนเป็นรากฐานในการค้นหาเขตอำนาจศาลของบุคคลในคดี International Shoe Co. v. Washington ซึ่งถูกเพิ่มเติมให้ละเอียดขึ้นโดยศาลในคดี Calder v. Jones. โดยศาลอุทธรณ์กล่าวย้ำเพิ่มเติมถึงความเห็นของศาลในคดี Bancroft & Masters, Inc. v. Augusta National Inc. ก่อนหน้านั้น ที่ศาลใช้ตีความคดี Calder ให้มีผลว่า "คดีนั้น(Calder) ไม่สามารถนำมาใช้กับปัญหาอย่างกว้างซึ่งการกระทำของต่างชาติ ด้วยผลที่อาจคาดการณ์ได้ในศาลของรัฐมักจะก่อให้เกิดเขตอำนาจศาลที่เฉพาะเสมอ" ศาลอุทธรณ์อ้างในคดี Bancroft เพิ่มเติมขณะตีความคดี Calder ว่า นอกเหนือหลักการเรื่องผลที่เกิดขึ้นแล้ว การกระทำที่ผิดกฎหมายของต่างชาติต้องมุ่งเป้าไปที่ศาลของรัฐโดยตรง อย่างไรก็ตาม ในคดี Yahoo! ศาลอุทธรณ์พบว่าการฟ้องร้องของ La Ligue Contre le Racisme et l'Antisemitisme's ต่อ Yahoo! ไม่ได้นับว่าเป็น "การมุ่งหมายโดยตรง" เนื่องด้วยคดีไม่มีคุณลักษณะว่า

---

[29] Frank B. Arenas, "Cyberspace Jurisdiction and the Implications of Sealand," Iowa Law Review 88, 1165 (2003) : 2.

การกระทำที่ผิดกฎหมายมีเป้าหมายที่ Yahoo! ขณะที่มีการถกเถียงกันถึงความถูกกฎหมายในการฟ้องคดีของ La Ligue Contre le et l'Antisemitisme ต่อ Yahoo! ศาลอุทธรณ์ก็พบว่า

LICRA and UEJF ฟ้องคดีเพื่อที่จะบังคับสิทธิทางกฎหมายของพวกเขาภายใต้กฎหมายฝรั่งเศส Yahoo! ไม่มีข้อกล่าวอ้างที่สามารถชักจูงศาลให้ลงความเห็นว่ามีสิ่งใดผิดกฎหมายในการกระทำขององค์กร เป็นผลให้ศาลเขตไม่ได้ใช้เขตอำนาจศาลทางบุคคลเหนือ LICRA and UEJF อย่างเหมาะสม เพราะว่าศาลเขตไม่มีเขตอำนาจศาลทางบุคคลเหนือคู่ความชาวฝรั่งเศส เราไม่ได้พิจารณาว่าการกระทำของ Yahoo! สำหรับการขอผ่อนผันตามประกาศครบกำหนดของการพิจารณาหรือไม่ หรือศาลเขตปฏิเสธอย่างเหมาะสมหรือไม่ที่ละเว้นจากการไต่สวนคดี

แม้ว่าศาลอุทธรณ์ปฏิเสธที่จะพิจารณาว่า การผ่อนพันตามประกาศครบกำหนดของการพิจารณาแล้วหรือไม่ แต่ศาลตั้งข้อสังเกตว่า ศาลสหรัฐฯ สามารถที่จะคาดการณ์เขตอำนาจศาล และสอบสวนข้ออ้างตาม First Amendment ได้ ถ้าองค์กรของฝรั่งเศสพยายามขอความช่วยเหลือจากศาลเขตสหรัฐฯ ในการบังคับคำตัดสินของฝรั่งเศส มันไม่อาจหลีกเลี่ยงได้ว่าองค์กรของฝรั่งเศสอาศัยศาลเขตของสหรัฐที่จะบังคับคำตัดสินของพวกเขา พวกเขาจะไม่ถูกบังคับใช้สิทธิก่อนโดยการฟ้องคดีของ Yahoo! ใช่หรือไม่ อย่างไรก็ตาม ไม่ว่าคำตัดสินของฝรั่งเศสจะผ่านชุมนุมของ First Amendment ในสภาวะที่ยังคงเป็นคำถามเปิดหรือไม่ก็ตาม อำนาจอย่างกว้างขวางของขอบเขตการพูดอย่างอิสระในสหรัฐฯ ก็ยังคงมีอยู่

ศาลอุทธรณ์มีคำสั่งให้มีการไต่สวนคดี Yahoo! ใหม่อย่างครบองค์คณะ ขณะที่โลกรอคอยคำตัดสินของคณะศาล มันทำให้เกิดข้อสงสัยขึ้นไปอีกว่า คำตัดสินของศาลฝรั่งเศสในคดี Yahoo! ก็ยังคงเปิดสำหรับการพิจารณาตาม First Amendment ซึ่งเป็นอันตรายอย่างเห็นได้ชัดต่อการบังคับใช้กฎหมายสแปมระหว่างประเทศ เพราะมันเป็นทิศทางที่นำไปสู่ข้อขัดแย้งอื่นๆ ที่เกี่ยวข้องกับอินเตอร์เนต อย่างไรก็ตาม ทั้งที่ความขัดแย้งกันทางกฎหมายเป็นอุปสรรค หลักการเรื่องถิ่นที่อยู่ก็เป็นวิธีแก้ปัญหาในทางปฏิบัติมากที่สุด ต่อปัญหาทางเลือกของศาลที่เกี่ยวกับเขตอำนาจศาล, กฎหมาย, และการบังคับใช้ในการจัดการกับสแปมในทางระหว่างประเทศ ตัวอย่างเช่น มันจะยอมให้ศาลสหรัฐฯ บังคับใช้ตามเงื่อนไขให้แสดงฉลากตามมาตรา 5(A)(i) และ 5(d)(1) เช่นเดียวกับเงื่อนไขอื่นๆ ของ CAN-SPAM Act ที่เกี่ยวข้องกับการส่งข้อความอิเล็กทรอนิกส์เชิงพาณิชย์โดยไม่ได้ร้องขอจากภายนอกสหรัฐฯ ในทางกลับกัน มันก็ยอมให้ประเทศอื่นๆ คาดเดาได้ถึงเขตอำนาจศาลต่อสแปมที่ส่งมา

จากสหรัฐฯ ที่ไม่ได้ปฏิบัติตามกฎของท้องถิ่น ความมีเหตุผลของคำตัดสินเช่นนี้ในสหรัฐฯ แน่นอนว่าอยู่ภายใต้ Due Process Clause ที่ถูกทำให้เห็นภาพโดยคดี Yahoo!

(2) First Amendment ตามรัฐธรรมนูญ เป็นเครื่องกีดขวางเงื่อนไขการมีฉลากบ่งว่าเกี่ยวกับเพศและการโฆษณาหรือไม่

First Amendment บัญญัติว่า "สภาคองเกรซควรจะทำให้ไม่มีกฎหมายที่พาดพิงถึงการก่อตั้งศาสนา หรือการห้ามการใช้สิทธิอย่างอิสระเช่นนั้น หรือลิดรอนเสรีภาพในการพูด (freedom of speech) หรือการเสนอข่าวสาร หรือสิทธิของประชาชนที่จะประชุม/ชุมนุมกันโดยสงบ และยื่นคำร้องต่อรัฐบาลเพื่อแก้ไขข้อข้องใจนั้น" สิทธิในการพูดอย่างอิสระตาม first amendment นั้น เป็นเครื่องมือป้องกันขั้นพื้นฐานสำหรับสิทธิในการสื่อสารออนไลน์ ซึ่งให้อำนาจอย่างกว้างขวางที่จะสื่อสารกับคนอื่นโดยปราศจากการแทรกแซงจากรัฐ

จุดยุ่งยากในการออกกฎหมายพื้นฐานสำหรับต่อต้านสแปมเมลมากที่สุดคือ การปกป้องของรัฐธรรมนูญที่มีต่อสแปมเมอร์เช่นเดียวกับกฎหมายที่ผูกมัดนักธุรกิจในการพูดเพื่อการพาณิชย์ First Amendment นั้นให้การป้องกันการพูดเพื่อการพาณิชย์ ถ้ามันเป็นกิจกรรมที่ถูกกฎหมายเป็นความจริง และไม่ก่อให้เกิดความเข้าใจผิด การโต้เถียงเรื่องสแปมเมลก็เช่นกัน ตั้งอยู่บนพื้นฐานของการพูดเชิงพาณิชย์ ซึ่งอยู่ในขอบเขตของกฎหมายที่เป็นอุปสรรคที่สำคัญอย่างเพียงพอในการบังคับใช้ CAN-SPAM Act

นักวิจารณ์ CAN-SPAM Act กล่าวหาว่ามาตราทั้งสองคือ 5(a)(5)(A)(i) และ 5(d)(1) ซึ่งต้องการให้มีฉลากบนข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอที่ชัดเจนและเห็นได้ชัดแจ้งโดยลำดับว่าเป็นโฆษณา และฉลากที่ให้คำแนะนำเกี่ยวกับเรื่องเพศ ซึ่งเป็นเงื่อนไขที่ไม่ได้มากไปกว่าการทำให้ "forced speech" ถูกต้องตามกฎหมาย ซึ่งเป็นความอ่อนแอของ First Amendment ในการปกป้องความศักดิ์สิทธิของเสรีภาพในการแสดงออก ข้อโต้แย้งนี้ได้รับการยืนยันจากโจทย์ที่ว่า กฎนี้น่าจะก่อให้เกิดภาระเกินควรต่อทั้งผู้มีสิทธิในการขายอุปกรณ์ทางเพศโดยผ่านข้อความอีเมล หรือผู้บริโภคที่รู้สึกสนใจในการซื้ออุปกรณ์ทางเพศที่เสนอถึงพวกเขาโดยผ่านข้อความอีเมล จริงๆ แล้ว การมีฉลากนั้นมีเจตนาเพื่อใช้กับการกลั่นกรองของ ISP ซึ่งกฎนี้อาจจะเป็นภาระต่อผู้ส่งอุปกรณ์ที่แนะนำเกี่ยวกับเพศอย่างถูกกฎหมาย

ดังนั้น ศาลสูงสหรัฐฯ จะตีความการต้องมีฉลากของ CAN-SPAM Act เผชิญหน้ากับ First Amendment อย่างไร หากศาลทราบดีว่าอินเตอร์เนต เป็นช่องทางการสื่อสารที่มีลักษณะเฉพาะประเภทหนึ่ง และยังทราบถึงความแตกต่างในแต่ละลักษณะช่องทางการสื่อสารด้วย และในทางประวัติศาสตร์ ได้ประยุกต์ใช้กฎไปตามชนิดของสื่อเพื่อทำให้แน่ว่าเงื่อนไขทางกฎหมายละเมิด First Amendment หรือไม่ จากคำตัดสินในคดี Reno และคดี Ashcroft ศาลสูงจะไม่อนุญาตให้ปิดกั้นการพูดอย่างอิสระบนอินเตอร์เนตอย่างไม่มีข้อสงสัย ดูจากแนวทางคดี Ashcroft ศาลซูพรีมอาจจะเผชิญหน้ากับความถูกต้องตามรัฐธรรมนูญของเงื่อนไขการมีฉลากโฆษณาของ CAN-SPAM Act ด้วยการสอบสวนไปในทางที่ว่ามีวิธีที่ก่อให้เกิดภาระน้อยลง หรือมีข้อจำกัดน้อยลงกว่าเงื่อนไขการมีฉลากหรือไม่ ที่สภาคองเกรซสามารถบรรลุเป้าหมายของตนในการให้อำนาจแก่ ISP และผู้รับอีเมลที่จะควบคุมข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอและข้อความที่ถูกแนะนำว่าเกี่ยวกับเพศ

นอกจากนั้น คำตัดสินของศาลสูงในคดี Rowan v. United States Post Office Department [30] ก็ได้เสนอมุมมองอื่นๆ ว่าศาลจะจัดการกับเงื่อนไขการมีฉลากของ CAN-SPAM Act อย่างไร ศาลในคดี Rowan ถือว่า First Amendment ไม่ได้ห้ามการบัญญัติกฎหมายของรัฐบาลกลางที่ยอมให้ผู้รับจดหมายถอนรายชื่อของตนออกจากบัญชีการส่งเมล และหยุดการรับเมลในอนาคตทั้งหมด ศาลกล่าวว่า "สิทธิที่จะสื่อสารของผู้ส่งเมลต้องหยุดลงที่กล่องจดหมายของผู้รับที่ไม่ต้อนรับ.....และเพื่อที่จะทำให้มีสแปมน้อยลงน่าจะเป็นการอนุญาตในรูปแบบของการล่วงล้ำเข้ามาได้" นี่ยืนยันถึงสิทธิทั่วไปของผู้รับที่จะยอมรับหรือปฏิเสธเมลที่ไม่ได้ร้องขอก็ได้ ในบริบทนี้ สิทธิในการพูดอย่างอิสระไม่ใช่เรื่องที่ทำได้แต่เพียงฝ่ายเดียว จากการศึกษา สิทธินี้ครอบคลุมถึงสิทธิของผู้รับที่ต้องการให้มีฉลากบนเมลที่ไม่ได้ร้องขอเท่านั้นอย่างมีเหตุผล จึงไม่ควรทำให้มีความแตกต่างว่าเงื่อนไขของกฎหมายตามคำสั่งของสภาคองเกรซ มีส่วนช่วยผู้รับอีเมล ปัจจัยสำคัญของเงื่อนไขการมีฉลาก ก็เพื่อให้แน่ใจว่ามีการแยกแยะข้อความโฆษณา และข้อความที่แนะนำเกี่ยวกับเรื่องเพศบนข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอ แม้ว่าเงื่อนไขการมีฉลากโดยผู้ส่งข้อความเช่นนั้น จะให้อำนาจทางเทคนิคแก่ ISPs และผู้รับกลุ่มเป้าหมายที่จะแยกแยะและกรองหรือห้ามข้อความเช่นนั้น การให้อำนาจเช่นนั้นก็ตกไปอย่างมีเหตุผลสนันสนุนภายในความเบาบางลงของคำตัดสินในคดี Rowan อันที่จริง ความหมายของ First Amendment ที่สร้างสรรค์ น่าจะสนับสนุนสิทธิของผู้รับอีเมลเชิงพาณิชย์

---

[30] Alongi, E. A. Has the U.S. Canned Spam?. Arizona Law Review 46, 263 (2004).

ที่ไม่ได้ร้องขอ ที่จะเลือกว่าข้อมูลแบบใดที่ยอมให้เข้ามากล่องจดหมายของพวกเขาได้ หรือกล่าวอีกนัยหนึ่งว่า ถ้า First Amendment รับรองเสรีภาพในการพูดของผู้ส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอ และอีเมลที่แนะนำเกี่ยวกับเรื่องเพศแล้ว มันควรจะรับรองเสรีภาพของผู้รับอีเมลที่ไม่ได้ร้องขอที่จะสมัครหรือคัดเลือกว่าอีเมลประเภทใด ที่จะอนุญาตหรือห้ามจากการส่งเข้ามาในกล่องจดหมายของพวกเขาเช่นเดียวกันด้วย เรื่องนี้ไม่ใช่ปัญหาใหม่ และอันที่จริงศาสสูงก็เห็นพ้องด้วย โดยผ่านคดีที่ไม่เกี่ยวพันกับสแปม

ยิ่งไปกว่านั้น ยังมีข้อโต้แย้งว่า "สิทธิที่ได้รับข้อความ ซึ่งสืบเนื่องมากจากสิทธิในการสร้างมันตามรัฐธรรมนูญ เป็นสิ่งที่แตกต่างกันอย่างชัดเจน และมีการบังคับใช้ทางกฎหมายที่เป็นอิสระจากกัน" ในคดี Virginia State Board of Pharmacy ศาสสูงถือว่า "เสรีภาพในการพูดนั้น "ปกป้องสิทธิที่จะรับอย่างเป็นธรรมดาอยู่เอง"" ศาสสูงให้ความเห็นเพิ่มเติมว่า; "เสรีภาพในการพูดแสดงถึงความตั้งใจของผู้พูด แต่ที่ผู้พูดยังมีอยู่อีก คือ การจัดหาการปกป้องอย่างเพียงพอต่อการสื่อสาร ทั้งต่อแหล่งข้อมูล และต่อผู้รับข้อความ" ความเห็นจากมุมมองที่ได้กล่าวมาข้างต้นนี้ จึงถูกต้องที่จะพิสูจน์ว่าเงื่อนไขการให้มีฉลากของ CAN-SPAM Act พยายามที่จะรักษาไว้ ซึ่งความสมดุลในระดับที่เท่าเทียมกันระหว่างสิทธิที่จะพูดอย่างมีอิสระของผู้ส่ง และผู้รับอีเมลเชิงพาณิชย์และเกี่ยวกับเพศ ตาม First Amendment อย่างสมบูรณ์เท่านั้น

ขณะที่คนสามารถคาดเดาได้เท่านั้นว่า ศาสสูงน่าจะตีความเงื่อนไขการมีฉลากของ CAN-SPAM Act โดยผ่าน First Amendment อย่างไร ศาลเขตทางตอนใต้ของโอไฮโอของสหรัฐฯ ในคำตัดสินคดี CompuServe เปิดช่องให้ตีความได้โดยตรงมากขึ้น และมองลึกซึ้งไปถึงว่าศาสสูงน่าจะจัดการกับเงื่อนไขการมีฉลากของ CAN-SPAM Act อย่างไร ศาลเขตถือว่า บริษัทที่โฆษณาทางอีเมลนั้น ไม่มีสิทธิในการพูดอย่างอิสระที่จะส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอถึงผู้ลงทะเบียนขอใช้บริการคอมพิวเตอร์ออนไลน์เชิงพาณิชย์ คำตัดสินบางส่วนถูกยืนยันได้จากหลักการในคดี Cyber Promotions [31] ซึ่งเป็นผู้ส่งอีเมลที่ไม่ได้ร้องขอ มีทางเลือกวิธีการสื่อสารอย่างเพียงพอที่สามารถหาได้ ซึ่งถูกนำมาอธิบายได้ดีกว่าด้วยคำกล่าวของศาลดังนี้

"การกระทำปัจจุบันของจำเลย มีทางเลือกในการสื่อสารที่เพียงพอที่สามารถหาได้สำหรับพวกเขา ไม่เพียงแต่พวกเขาจะมีอิสระที่จะส่งโฆษณาทางอีเมลถึงใครบนอินเตอร์เนตที่ไม่ได้ใช้

---

[31] Ibid p. 5-6.

บัญชีเมลของ Compuserve เท่านั้น แต่พวกเขายังสามารถสื่อสารกับสมาชิกของ Compuserve ได้เช่นเดียวกัน โดยผ่านกระดานข่าวออนไลน์, การโฆษณาทางเวปเพจ, หรือวิธีการส่งแฟกซ์ เช่นเดียวกับโดยผ่านวิธีที่เป็นแบบดั้งเดิมมากขึ้น เช่น การส่งจดหมาย หรือการตลาดทางโทรศัพท์ ข้อต่อสู้ของจำเลยที่อ้างถึงต้นทุนที่ต่ำของสื่ออีเมล ว่าไม่มีวิธีการสื่อสารที่เป็นทางเลือกอย่างเพียงพอนั้น เป็นสิ่งที่ไม่อาจจูงใจให้เชื่อได้ ไม่มีเงื่อนไขใดๆ ตามรัฐธรรมนูญ ที่ต้นทุนที่เพิ่มขึ้นจากการส่งโฆษณาที่ไม่ได้ร้องขอปริมาณมากๆ ต้องถูกแบกรับโดยผู้รับ"

ในบริบทของคดี CompuServe ผู้ส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอที่ไม่ชอบเงื่อนไขการให้มีฉลาก ไม่ควรมีสิทธิการพูดอย่างอิสระที่ส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอ เพราะว่าโดยส่วนมากพวกเขามีวิธีการสื่อสารที่เป็นทางเลือกอย่างเพียงพอแน่นอน ถึงผู้ฟังที่เป็นกลุ่มเป้าหมายของพวกเขา ถ้าไม่มีสิทธิในการพูดอย่างอิสระที่ส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอ หรืออีเมลที่มุ่งไปในเรื่องเพศแล้ว ก็จะไม่มีสิทธิการพูดอย่างมีอิสระ ที่ถูกคุกคามโดยเงื่อนไขการมีฉลากของ CAN-SPAM Act อย่างเป็นเหตุเป็นผล เมื่อดูจากมุมมองนี้ มันสามารถพิสูจน์ได้ว่าเงื่อนไขการมีฉลากนั้นไม่ได้เป็น "forced speech" อย่างสมบูรณ์ ดังนั้นจึงไม่ได้ละเมิด First Amendment ปัญหาในเรื่องนี้เสริมด้วยข้อเท็จจริงที่ว่า การต้องการให้มีฉลากไม่ใช่การห้ามข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอหรือข้อความที่มุ่งเกี่ยวกับเรื่องเพศที่ไม่ได้ร้องขอไปทั่ว แต่กำหนดเงื่อนไขเพียงเล็กน้อยเท่านั้น ในการส่งข้อความอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอ ที่ทั้งก่อให้เกิดภาระทางเศรษฐกิจที่เพิ่มขึ้น และรุกล้ำความเป็นส่วนตัวของผู้รับ

C. เงื่อนไขการมีข้อความจั่วหัวที่แท้จริง ลิทธิที่จะไม่แสดงตัวของ CAN-SPAM Act (Accurate Header Provision and the Right to Anonymity)

มาตรา 5(a)(1) ของ CAN-SPAM Act ห้ามการส่งข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอ ซึ่งข้อมูลจั่วหัวนั้นหลอกลวงในเนื้อหา หรือทำให้เกิดความเข้าใจผิดในเนื้อหา กฎหมายยังกำหนดให้ชัดเจนไปด้วยถึงชนิดของข้อมูลจั่วหัวที่น่าจะถูกจัดกลุ่มเช่นนั้น ยิ่งไปกว่านั้น กฎหมายในมาตรา 3(8) นิยาม "header information" ว่าหมายถึง "แหล่งกำเนิด, ปลายทาง, เส้นทางข้อมูลที่ติดมากับข้อความอีเมล รวมถึงโดเมนเนมของต้นทาง และที่อยู่อีเมลของต้นทาง และข้อมูลอื่นใดที่ปรากฏบนบรรทัดในการแสดงตัว หรือชวนให้เข้าใจว่าเป็นการแสดงตัวบุคคลที่ริเริ่มข้อความนั้น" เงื่อนไขข้างต้นมีผลเป็นการเปิดเผยตัวตนออนไลน์ของผู้ส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขออย่างไม่อาจจะหลีกเลี่ยงได้ ซึ่งก่อให้เกิดความกังวลในหมู่ผู้สนับสนุนสิทธิเอกชน ว่าเงื่อนไข

ดังกล่าวอาจจะเป็นอันตรายต่อความต้องการปกปิดตัวตน (anonymity) และการสื่อสารที่ไม่อยากเปิดเผยบนอินเตอร์เนต คำถามที่ตรงกับปัญหาคือ ศาลสหรัฐฯ จะถือว่าเงื่อนไขการมีข้อมูลจั่วหัวที่แท้จริงของ CAN-SPAM Act ละเมิด First Amendment หรือไม่ คำถามนี้จะถูกตอบในบริบทของสิทธิที่จะสื่อสารโดยไม่แสดงตัว

ศาลสหรัฐฯ รับรองถึงสิทธิตามรัฐธรรมนูญโดยทั่วๆ ไป ที่จะพูดโดยไม่แสดงตัว ในคดี McIntyre v. Ohio Elections Commission ศาลซูพรีมแสดงตัวร่วมด้วย และสนับสนุนการปกปิดตัวตนในฐานะที่เป็นเหมือนรากฐานของเสรีภาพในการพูดที่ไม่อาจแบ่งแยกได้ภายใต้ First Amendment ตามรัฐธรรมนูญ

คำตัดสินที่สนับสนุนการไม่แสดงตัวตนนั้น อาจจะถูกกระตุ้นโดยความเกรงกลัวทางเศรษฐกิจ หรือการแก้แค้นอย่างเป็นทางการ หรือโดยความกังวลว่าจะถูกคว่ำบาตรทางสังคม หรือโดยความปรารถนาที่จะสงวนไว้ซึ่งความเป็นส่วนตัวให้มากที่สุดเท่าที่จะเป็นไปได้เพียงเท่านั้น ไม่ว่าแรงจูงใจจะเป็นอะไรก็ตาม อย่างน้อยในขอบเขตของความพยายามทางอักษรศาสตร์ ประโยชน์จากการมีผลงานที่ไม่เปิดเผยตนเข้าไปในตลาดทางความคิด ก็มีน้ำหนักกว่าผลประโยชน์สาธารณะใดๆ ที่ต้องการการเปิดเผยตัวตนเสมือนเป็นเงื่อนไขในการเข้าไปอย่างไม่มีข้อสงสัย ฉะนั้นการตัดสินใจของผู้เขียนที่จะคงไว้ซึ่งการปกปิดตัวตน เช่นเดียวกับการตัดสินใจอื่นๆ ที่เกี่ยวข้องกับการละเว้น หรือการเพิ่มเติมในเนื้อหาของสิ่งพิมพ์ ก็เป็นหลักเกณฑ์ของเสรีภาพในการพูดที่ได้รับการปกป้องตาม First Amendment

ในฐานะสื่อกลางของการสื่อสาร เวปอยู่ภายใต้การจับตามองของศาลในการกำหนดลักษณะ, ระดับ, และขอบเขตของการไม่แสดงตนที่สามารถยอมให้ได้ Anne Wells Branscomb [32] เสนอว่า การปกปิดตัวตนที่แท้จริงบนเวป "หมายว่าไม่มีใครสามารถที่จะแกะรอยแหล่งกำเนิดข้อความอิเล็กทรอนิกส์ได้" Branscomb อ้างเหตุผลเพิ่มเติมว่า First Amendment ไม่อนุญาตให้มีการห้ามการปกปิดตัวตนที่แท้จริง ถึงขนาดที่ว่าการแทรกแซงรัฐบาลด้วยข้อความสนเท่ห์นั้นผิดกฎหมายก็ตาม การไม่เปิดเผยตัวตนบนอินเตอร์เนตทำให้เกิดข้อได้เปรียบอย่างยิ่ง ขณะที่ยอมรับถึงข้อด้อยของมันที่จะถูกนำไปใช้ในทางที่ผิด Raymond S.R. Ku และผู้เขียนร่วมก็ให้ความเห็นว่า การปกปิดตัวตนบนไซเบอร์สเปซโดยการใช้ชื่อปลอม และนามแฝงอาจจะช่วยกำจัดการแบ่งแยกที่ต่อต้านสตรี และชนกลุ่มน้อยได้

---

[32] Taiwo A. Oriola, p.13.

อย่างไรก็ตาม การปกปิดตัวตนอย่างแท้จริงมีนัยที่สำคัญต่อสังคมไซเบอร์ เนื่องจากข้อด้อยของมันที่จะถูกนำไปใช้ในทางที่ผิด ในบริบทของอีเมลที่ไม่ได้ร้องขอ การปกปิดตัวตนที่แท้จริงน่าจะเป็นการสนับสนุนให้มีการส่งข้อมูล ซึ่งหัวอีเมลนั้น ก่อให้เกิดความใจผิดในสาระสำคัญ หรือเป็นการหลอกลวง ตัวอย่างเช่น อุปกรณ์ที่แนะนำเรื่องเพศอาจจะมากับข้อมูลจั่วหัวที่แสดงให้เห็นว่าเป็นการโฆษณา การขายสินค้าที่เกี่ยวกับบ้าน หรือนโยบายการให้ประกัน ผลก็คือ อิสระภาพของผู้รับ หรือสิทธิที่จะควบคุมบรรยากาศทางอิเล็กทรอนิกส์ของตัวเองก็จะตกอยู่ในอันตราย ด้วยไม่มีใครสามารถให้ความเห็นหรือสามารถรับผิดชอบได้ เนื่องจากการปกปิดตัวตนอย่างไม่มีข้อผูกมัดใดๆ ในคดี Miller ศาลเขตสหรัฐฯ ทางตอนเหนือของจอร์เจีย ยอมรับในวัตถุประสงค์เบื้องต้นของกฎหมายที่ห้ามการฉ้อโกงของรัฐ ในฐานะที่เป็นผลประโยชน์ของรัฐที่ไม่อาจขัดขืนได้ ซึ่งสามารถลบล้างการปกปิดตัวตนบนเวปได้ อย่างไรก็ตาม ศาลประกาศว่ากฎหมายนี้ไม่ชอบด้วยรัฐธรรมนูญ เพราะว่ากฎหมายไม่ได้ถูกออกแบบมาอย่างแคบเพื่อให้บรรลุถึงเป้าหมายในที่สุด และได้กวาดต้อนผู้บริสุทธิ์ซึ่งการพูดได้รับการปกป้องภายในขอบเขตของกฎหมายไปแทน โดยเฉพาะในภาษาที่เรียบง่ายของมัน ข้อห้ามในทางอาญานำมาปรับใช้โดยไม่คำนึงถึงว่าผู้พูดมีเจตนาใดๆ หรือไม่ที่จะหลอกลวง หรือมีการหลอกลวงเกิดขึ้นอย่างแท้จริงหรือไม่ ดังนั้น มันอาจจะนำไปใช้ในขอบเขตอย่างกว้างมาก ในการส่งอีเมลที่แสดงตัวผู้ส่งอย่างผิดๆ (falsely identify) แต่ไม่เป็นการฉ้อโกง (fraudulent) ตามความหมายที่เฉพาะเจาะจงในทางกฎหมายอาญา

ผลจากคดี Miller ทำให้สิทธิในการปกปิดตัวตนนั้นไม่สมบูรณ์ แต่สามารถนำมาใช้อย่างจำเป็น โดยป้องกันการหลอกลวง หรือโดยกฎหมายที่มุ่งเน้นถึงผลประโยชน์สาธารณะอื่นๆ โดยจัดให้กฎหมายเช่นนั้นถูกออกแบบมาอย่างแคบ เพื่อให้บรรลุถึงเป้าหมายนั้น โดยปราศจากการเหยียบย่ำการพูดที่ได้รับการปกป้องที่บริสุทธิ์ ทั้งนี้ จุดมุ่งหมายเบื้องต้นของมาตรา 5(a)(1) ของ CAN-SPAM Act คือการห้ามใช้ข้อมูลจั่วหัวที่ก่อให้เกิดความเข้าใจผิดโดยการหลอกลวงในอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอ ซึ่งเป็นผลประโยชน์สาธารณะที่ไม่อาจขัดขืนได้โดยปราศจากข้อสงสัย ยิ่งไปกว่านั้น มาตรานี้ไม่ได้นำไปประยุกต์ใช้กับรูปแบบของอีเมลทุกประเภท แต่นำไปประยุกต์ใช้กับอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอเท่านั้น ดังนั้น เงื่อนไขนี้จึงถูกกำหนดมาอย่างแคบ และไม่น่าจะมีผลต่อข้อความอิเล็กทรอนิกส์ที่ไม่ได้ร้องขอที่ไม่ใช่ในเชิงพาณิชย์ จึงไม่กระทบต่อสิทธิในการพูดอย่างอิสระของผู้ใช้อินเตอร์เนตโดยทั่วไป ที่ส่งข้อความอิเล็กทรอนิกส์ที่ไม่ใช่ในทางพาณิชย์ที่ไม่ได้ร้องขอเป็นประจำ เมื่อมองจากมุมมองนี้แล้ว มาตรา 5(a)(1) ของ CAN-SPAM Act จึงผ่านข้อโต้แย้งตาม First Amendment ไปอย่างมีเหตุผล

ยิ่งไปกว่านั้น เพื่อที่จะให้แน่ใจว่าศาลสหรัฐฯ จะแปลความหมายเงื่อนไขข้อมูลจั่วหัวที่แท้จริงในมาตรา 5(a)(1) ของ CAN-SPAM Act อย่างไร จึงเป็นการสมควรที่จะวิเคราะห์เชิงเปรียบเทียบ แม้แต่ในกฎหมายที่ไม่เกี่ยวกับสแปมที่บัญญัติในเรื่องการปกปิดตัวตนในการสื่อสาร ในคดี Talley v. California ผู้ฎีกาถูกดำเนินคดีในข้อหาละเมิดเทศบัญญัติของเมือง ซึ่งห้ามการแจกจ่ายใบปลิวสนเท่ห์ในสถานที่ และภายใต้สถานการณ์ใดๆ ก็ตาม ผู้ฎีกาแจกใบปลิวจำนวนหนึ่งซึ่งกระตุ้นให้ผู้อ่านคว่ำบาตรธุรกิจบางกลุ่ม ที่ขายสินค้าที่ผลิตโดยบริษัทที่กีดกันเชื้อชาติต่อโอกาสในการจ้างงานของพวกเขา ในการยกเลิกเทศบัญญัติของแคลิฟอร์เนียเพราะละเมิด Fourteenth and First Amendments ผู้พิพากษา Black ได้บันทึกไว้ว่า

"ไม่น่าจะมีปัญหาว่าความต้องการให้แสดงตนเช่นนั้นจะนำไปสู่เสรีภาพที่จำกัดที่จะแพร่กระจายข้อมูล และโดยเช่นนั้นเป็นการจำกัดซึ่งเสรีภาพที่จะแสดงออก "เสรีภาพในการแพร่หลาย เป็นสิ่งที่จำเป็นต่ออิสรภาพนั้น เท่าๆ กับเสรีภาพในการดีพิมพ์ อันที่จริง ถ้าปราศจากการแพร่หลายแล้ว สิ่งพิมพ์ก็จะมีคุณค่าเพียงเล็กน้อยเท่านั้น" หนังสือเล่มเล็ก, ใบปลิว, โบรชัวร์ และแม้แต่หนังสือสนเท่ห์เหล่านี้ แสดงบทบาทที่สำคัญต่อความก้าวหน้าของมนุษย์ชาติ กลุ่มและนิกายที่ถูกประหารจากรุ่นสู่รุ่นโดยผ่านประวัติศาสตร์อันยาวนาน สามารถที่จะวิเคราะห์ได้ถึงการกระทำและกฎหมายที่กดขี่ ทั้งที่ไม่แสดงตัว หรือไม่ก็ตาม"

โดยอ้างถึงคำตัดสินก่อนๆ ของศาล ในคดี Bates v. City of Little Rock และคดี NAACP v. Alabama ศาลซูพรีมในคดี Talley อ้างเพิ่มเติมว่า

"เรามีโอกาสเมื่อเร็วๆ นี้ ที่จะหยิบยกเอาสองคดี ที่มีช่วงเวลาและพฤติการณ์ เมื่อรัฐไม่อาจจะบังคับสมาชิกของรัฐ ให้ผูกมัดในการแพร่กระจายความคิดที่จะแสดงตนต่อสาธารณะ เหตุผลต่อคำกล่าวอ้างเช่นนั้นคือว่า การแสดงตน และความกลัวต่อการถูกแก้แค้นเอาคืนอาจจะเป็นอุปสรรคต่อการวิพากษ์วิจารณ์เหตุการณ์สาธารณะที่สำคัญโดยสงบสุขอย่างแน่นอน เทศบัญญัติของคณะกรรมการลอสแองเจลิสนี้ อยู่ภายใต้ความบกพร่องเดียวกันนี้ เราถือว่ามันเป็นเช่นเดียวกับเทศบัญญัติของกริฟฟิน และจอร์เจีย คือเป็นโมฆะในแง่นั้น"

แม้ว่าคำตัดสินในคดี Talley จะเอาชนะเทศบัญญัติของแคลิฟอร์เนียซึ่งบังคับสิทธิของผู้ฎีกาที่จะติดต่อสื่อสารโดยไม่แสดงตน ตามที่ได้รับการรับรองโดย the First and Fourteenth Amendments ได้ แต่เทศบัญญัติของแคลิฟอร์เนียที่มีขอบเขต และมาตรา 5(a)(1) ของ CAN-SPAM Act ที่ต้องการข้อมูลจั่วหัวที่แท้จริงในการส่งข้อความอิเล็กทรอนิกส์ ก็ไม่มีทางที่จะ

สามารถนำมาเปรียบเทียบกันได้ มาตรา 28.06 ในเทศบัญญัติเมืองฉบับที่ 77,000 ของเมืองลอส แองเจลลีส ที่ถูกโจมตีโดยศาลคดี Talley กำหนดว่า

ห้ามบุคคลใดแจกจ่ายใบปลิวใดๆ ก็ตาม ในสถานที่ใดๆ ก็ตาม ภายใต้สถานการณ์ใดๆ ก็ตาม ที่ไม่มีการพิมพ์บนปก หรือด้านหน้าของใบปลิวนั้น ถึงชื่อและที่อยู่ ตามนี้

(1) บุคคลที่พิมพ์, เขียน, รวบรวม หรือผลิตใบปลิวเช่นนั้น

(2) บุคคลที่เป็นสาเหตุให้ใบปลิวนั้นถูกแจกจ่าย; จัดเตรียมให้ อย่างไรก็ตาม ในกรณีที่เป็นชื่อบุคคล หรือสโมสรที่แต่งขึ้น ต้องเพิ่มเติมถึงชื่อที่แต่งขึ้นเช่นนั้น ด้วยชื่อที่แท้จริงและที่อยู่ของเจ้าของ ผู้จัดการหรือเจ้าหน้าที่ของบุคคลที่สนับสนุนการทำใบปลิวเช่นนั้นควรจะปรากฏบนไปปลิวนั้นด้วย

ในทางตรงกันข้าม ประเภทของการพูดที่ถูกนำมาบัญญัติโดยมาตรา 5(a)(1) ของ the CAN-SPAM Act คือ ข้อความที่ไม่เกี่ยวกับการเมืองเป็นสาระสำคัญ และเป็นการโฆษณาเชิงพาณิชย์ที่มุ่งเป้าหมายไปที่บุคคลที่จะเป็นลูกค้าในอนาคต ผู้ส่งข้อความเชิงพาณิชย์ที่ไม่ได้ร้องขอเช่นนั้นที่ถูกต้องการอย่างแท้จริง ให้มีข้อมูลจั่วหัวที่เป็นจริง และเชื่อถือได้บนข้อความอิเล็กทรอนิกส์ที่ไม่ได้ร้องขอของพวกเขา แม้ว่าเงื่อนไขมีผลเป็นการเปิดเผยตัวตนที่แท้จริงของผู้ส่ง ซึ่งเป็นผลให้แวดล้อมด้วยพฤติการณ์ที่บริสุทธิ์ใจ และ (ไม่เหมือนกับคดี Talley) แทบจะไม่ก่อให้เกิด "ความกลัวต่อการแก้แค้น" ที่อาจจะเป็นอุปสรรคต่อการวิพากษ์วิจารณ์เหตุการณ์สาธารณะที่สำคัญโดยสงบสุขอย่างแน่นอน ข้อเสียที่อาจจะเกิดขึ้นต่อข้อความเช่นนั้นคือ ความชัดเจนที่เพิ่มมากขึ้น และความอ่อนแอของเทคโนโลยีการกรองข้อความ ที่จะทำให้มันง่ายขึ้นต่อ ISPs และผู้รับที่จะลบข้อความอันเป็นสิทธิในการรับรู้อย่างมีเหตุผลภายใต้ the First Amendment

จากบทวิเคราะห์ที่กล่าวมาทั้งหมดอาจสรุปได้ว่า CAN-SPAM Act อาจต้องเผชิญหน้ากับความท้าทายอย่างใหญ่หลวงในการคาดหวังถึงความสำเร็จของมันในเรื่อง ข้อกล่าวห้าเรื่องการละเมิด First and Fourteenth Amendments เรื่องเงื่อนไขการมีฉลากและการให้ข้อมูลหัวเรื่องที่แท้จริง ซึ่งอาจเกิดขึ้นได้ เพราะเป็นการทำลายสิทธิในการสื่อสารโดยไม่แสดงตน อย่างไรก็ดี ศาลก็น่าจะมีทางออกจากตัวอย่างคำพิพากษาที่ได้ยกมาแล้วว่า บทกฎหมายนี้มีเหตุผลในการรักษาไว้ซึ่งความสมดุลที่เท่ากัน ระหว่างสิทธิที่ขัดแย้งกันของผู้ส่งข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอ และผู้รับที่เป็นกลุ่มเป้าหมายของพวกเขา ทฤษฎีก้าวหน้าไปถึงว่าผู้ส่งข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอไม่อาจอ้างถึงการปกป้องการพูดอย่างอิสระตาม First Amendment ได้มากไปกว่าผู้รับ

ข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอที่มีสถานะในการกำหนดเงื่อนไขสำหรับการได้รับข้อความเช่นนั้น ดังนั้น อาจจะกล่าวได้ว่าศาลสหรัฐมีความเป็นไปได้มากที่สุดที่จะปลดเปลื้อง CAN-SPAM Act จากการละเมิดการพูดอย่างอิสระใดๆ

นอกจากนี้ ข้อดีโดยธรรมชาติในการบังคับใช้ก่อนของ CAN-SPAM Act ต่อกฎหมายสแปมของรัฐ พบว่าข้อดีต่อความกลัวของคองเกรซว่ากฎหมายสแปมของรัฐที่ไม่เหมือนกันอาจจะก่อให้เกิดความสับสนระหว่างพลเมืองที่ต้องผูกพันตามกฎหมายนั้น จึงเป็นเหตุผลให้สิทธิในข้อยกเว้นต่อกฎหมายรัฐบาลกลางในกฎหมายสแปมของรัฐน่าจะทำให้ง่าย เป็นรูปแบบเดียวกัน และก่อให้เกิดความร่วมมือกันที่ดีกว่าในการต่อสู้กับสแปม และสิ่งที่สำคัญมากที่สุด ก็คือสิทธิในการบังคับใช้ก่อนน่าจะลบล้างการปะทะกันอย่างหลีกเลี่ยงไม่ได้ของกฎหมายสแปมของรัฐกับรัฐธรรมนูญของสหรัฐฯ ในเงื่อนไขด้านการพาณิชย์ หากรัฐดำเนินการตามกฎหมายต่อการละเมิดกฎหมายสแปมระหว่างรัฐ

การบังคับใช้กฎหมายสแปมระหว่างประเทศ ก็เป็นอุปสรรคสำคัญอย่างหนึ่งต่อความสำเร็จของ CAN-SPAM Act อันขาดซึ่งธรรมเนียมปฏิบัติระหว่างประเทศเรื่องเกี่ยวกับเขตอำนาจศาล และการบังคับคำตัดสินต่างชาติในข้อขัดแย้งที่เกี่ยวกับอินเตอร์เนต สหรัฐฯ น่าจะมีความหวังในผลประโยชน์ตอบแทนร่วมกันในการบังคับใช้กฎหมายสแปมระหว่างประเทศ ซึ่งอาจไม่ใช่เรื่องง่าย เพราะต้องบังคับใช้คำตัดสินต่างชาติในท้องถิ่นในสหรัฐฯ อุปสรรคในการบังคับใช้คำตัดสินต่างชาติในสหรัฐฯ ถูกทำให้เป็นขั้นตอนมากขึ้นโดยกระบวนการการบังคับตามกฎหมายของ the Fourteenth Amendment ประเด็นนี้ถูกนำมาอธิบายได้อย่างดีโดยคดี Yahoo ดังนั้น ไม่มีประเทศต่างชาติใดๆ จะบังคับคำตัดสินของศาลสหรัฐที่เกี่ยวกับ CAN-SPAM Act ได้ ถ้าไม่มีการประกันถึงผลตอบแทนอย่างเดียวกันจากศาลสหรัฐฯ ทางออกที่ดีที่สุดอาจจะเป็นการฟื้นคืนมาของการพิจารณาข้อเสนอ the proposed Hague Convention on International Jurisdiction and Foreign Judgments in Civil and Commercial Matters.

CAN-SPAM Act ยังไม่ใช่สิ่งที่สมบูรณ์อย่างแท้จริง ข้อด้อยที่ว่าปัจเจกชนไม่ได้รับอนุญาตให้ฟ้องคดีแพ่งสำหรับข้อกล่าวหาว่าละเมิดบทบัญญัติของกฎหมาย ยิ่งไปกว่านั้น กฎหมายยังรับเอารูปแบบ "opt-out" มาใช้ในการส่งสแปม ซึ่งเป็นที่เข้าใจโดยทั่วๆ ไปว่ามีความหละหลวมมากกว่ารูปแบบที่มีพื้นฐานบนความยินยอมแบบ "opt-in" ซึ่งกฎหมายสแปมของบางรัฐให้ความสนับสนุน อย่างไรก็ตาม การประเมินข้อด้อยของกฎหมายควรจะพิจารณาถึงความจำเป็นต่อการติดต่อสื่อสารด้าน

อีคอมเมิรซ์ที่ไม่ถูกปิดกั้น และยังมีความยุ่งยากของ First and Fourteenth Amendment ตามรัฐธรรมนูญ ซึ่งประสบความสำเร็จในการทำลายความพยายามครั้งก่อนๆ ของสภาคองเกรซที่จะออกกฎหมายอินเตอร์เนต ดังนั้น กฎหมายต่อต้านสแปมที่แข็งแรงกว่า CAN-SPAM Act จึงสิ้นสุดลงโดยการยืดฉวยไว้ของ First Amendment นั่นเอง

3.4.5 ข้อพิพาท คำวินิจฉัย และประเด็นทางกฎหมายอื่นๆ ที่เกิดจากการส่งจดหมายอิเล็คทรอนิคส์ที่ผู้รับมิได้ยินยอม

ก่อนที่สหรัฐอเมริกาจะมีการตรา CAN SPAM Act of 2003 ออกมาใช้บังคับเมื่อต้นปี 2004 ผู้บริโภคและผู้ให้บริการอินเตอร์เนตในรัฐต่างๆ ในสหรัฐอเมริกา ได้มีความพยายามที่จะจัดการกับปัญหาสแปมเมลตลอดมา เท่าที่กฎหมายจะสามารถเอื้ออำนวยได้ โดยในส่วนของผู้บริโภคเองก็พยายามใช้มาตรการหลายอย่างๆ เพื่อลดจำนวนสแปมเมลลง ทั้งการลดสแปมเมล การใช้โปรแกรมกรองสแปมเมล การเปลี่ยนอีเมลแอดเดรส และการพยายามรักษาความเป็นส่วนตัวของอีเมล ในส่วนของผู้ให้บริการอินเตอร์เนตเอง (ISP) ก็พยายามที่จะใช้ข้อตกลงการให้บริการที่ห้ามการส่งสแปม ใช้โปรแกรมในการตรวจจับและหยุดสแปมเมล และมาตรการทางกฎหมาย

ผู้ให้บริการอินเตอร์เนตหลายรายพยายามที่จะหยุดสแปมเมอร์โดยการฟ้องร้องคดีเกี่ยวกับสแปมเมลหลายคดี ภายใต้ข้อกฎหมายที่มีอยู่ ดังต่อไปนี้

3.4.5.1 การละเมิดสังหาริมทรัพย์ (Tresspass to Chattels)

ประเด็นในเรื่องการละเมิดสังหาริมทรัพย์ถือเป็นประเด็นหนึ่งที่นำมาใช้จัดการกับสแปมเมล โดยผู้ให้บริการอินเตอร์เนตต้องรับภาระทางเศรษฐกิจในการจัดการกับสแปมเมล เนื่องจากทราฟฟิคอีเมลที่ช้าลง, เซิร์ฟเวอร์ต้องรับภาระหนักขึ้น และความเสี่ยงต่อการสูญเสียผู้รับบริการ แต่ผลของคดีก็ยังมีความหลากหลาย เหล่านี้เป็นตัวอย่างคดีของสหรัฐฯ ในเรื่องนี้ เช่นในแคลิฟอร์เนียคดี Ferguson v. Friendfinders ศาลอุทธรณ์ยกฟ้องข้ออ้างในประเด็นเรื่องการละเมิดสังหาริมทรัพย์ เนื่องจากโจทก์ไม่สามารถพิสูจน์ถึงความเสียหายที่แท้จริงได้

เช่นเดียวกับคดี Intel v. Hamidi [33] ซึ่งถูกตัดสินโดยศาลซูพรีมของแคลิฟอร์เนีย อันแสดงให้เห็นว่าข้อโต้แย้งเรื่องการละเมิดในไซเบอร์สเปซนั้นไม่ใช่เรื่องใหม่ อัน

---

[33] "Trespass to Chattels and the Internet: Intel v. Hamidi," Harvard Journal of Law & Technology 17, 283 (2003) : 1-3.

ก่อให้เกิดความคิดที่ขัดแย้งกันระหว่างผู้พิพากษา โดยสรุปคือ กล่าวว่า Intel ล้มเหลวที่จะอ้างถึงการละเมิดอสังหาฯ เพราะอินเทลไม่สามารถที่จะอธิบายได้ว่าการละเมิดของมัน (ระบบคอมพิวเตอร์) ก่อให้เกิดความเสียหายอย่างไร แม้ว่า อินเทล ต่อสู้ว่าการมีความเสียหายนั้นไม่มีความจำเป็น เพราะว่ามันหาวิธีการบรรเทาความเสียหายได้ – ข้อโต้แย้งที่ยกขึ้นในวันที่มีการอุทธรณ์นั้น ศาลซูพรีมของรัฐพิจารณาเหตุผลของอินเทลว่าไม่สมเหตุสมผล "ประเด็นเรื่องการเยียวยาโดยปราศจากการแสดงถึงความเสียหายที่แก้ไขไม่ได้ในการกระทำละเมิดสังหาฯ ซึ่งความเสียหายต่อทรัพย์สินส่วนบุคคล หรือผลประโยชน์ของผู้ครอบครองนั้น ***เป็น*** อันเป็นองค์ประกอบพื้นฐานของการกระทำ น่าจะทำให้เกิดผลทางกฎหมายเพียงเล็กน้อยเท่านั้น" อินเทลจะพิสูจน์อย่างไรว่าทุกครั้งที่ Hamidi ส่งข้อความอีเมลนั้น มี Hamidi ที่มากขึ้นอีกสิบรออยู่ในความเสียหายที่แท้จริง แต่ Intel ก็ไม่สามารถพิสูจน์ได้ถึงความเสียหายที่เกิดขึ้นกับทรัพย์สินของตนเองได้ ถึงแม้ว่า Hamidi ซึ่งเคยเป็นพนักงานของ Intel มาก่อนได้พยายามส่งอีเมลจำนวน 200,000 ฉบับถึงพนักงานของ Intel เพื่อเป็นการก่อกวนการทำงานของพนักงานของ Intel และพยายามทำลายระบบ Computer Network ของ Intel

การละเมิดสังหาริมทรัพย์ดูเหมือนจะประสบความสำเร็จมากกว่าภายใต้กฎหมายของรัฐเวอร์จิเนีย และโอไฮโอ เช่นในคดีของ AOL v. Joseph Melle[34] ในเขตตะวันออกของรัฐเวอร์จิเนีย โดยศาลพบว่า Melle ส่งอีเมลโฆษณาจำนวนกว่า 6 ล้านฉบับถึงสมาชิกของ AOL โดยไม่ได้รับอนุญาต โดยยังคงทำการส่งอย่างต่อเนื่องแม้ว่าจะได้รับการแจ้งให้หยุดการส่งอีเมลเหล่านั้นจาก AOL แล้วก็ตามที ผลจากการส่งอีเมลจำนวนมากเหล่านี้ทำให้ AOL ต้องทำการขยายเครือข่าย และเวลาการทำงานของพนักงานเพื่อป้องกันสมาชิกและระบบคอมพิวเตอร์ จากการโจมตีของสแปมเมล

ในปี 2001 ในคดี ระหว่าง AOL v. National Care Discount,Inc. (NHCD) ภายใต้กฎหมายของรัฐเวอร์จิเนีย โดยศาลพบว่า (NHCD) ต้องรับผิดต่อในการกระทำภายใต้สัญญาที่มีต่อผู้ให้บริการ และถือว่าการกระทำของ (NHCD) เป็นการละเมิดสังหาริมทรัพย์ โดยศาลพิพากษาให้ AOL ได้รับการชดใช้ค่าเสียหายเป็นจำนวน 2.5 เหรียญ ต่อหนึ่งพันอีเมล จากจำนวน 135 ล้านอีเมลที่ถูกส่ง รวมเป็นเงินทั้งหมด 337,500 ดอลล่าห์สหรัฐรวมดอกเบี้ยและค่าทนายความด้วย

คดีที่น่าสนใจอีกเรื่องหนึ่งเกิดขึ้นในรัฐโอไฮโอ คือคดีระหว่าง CompuServe v. Cyber Promotions[35] ในประเด็นเรื่องการละเมิด โดยศาลกล่าวว่า โจทก์ สามารถยกประเด็นเรื่อง

---

[34] Ibid p,6-7..

[35] Ibid p,5-7.

การละเมิด โดยไม่มีอำนาจและสิทธิที่จะเข้าครอบครอง ศาลพิจารณาจากพยานต่างๆ แล้วเห็นว่า มูลค่าความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ของโจทก์ทั้งหมดนั้นเกิดขึ้นจากการที่ต้องขยายช่องสัญญาณเพื่อให้เพียงพอต่อความต้องการของลูกค้า และการจัดการกับอีเมลจำนวนมหาศาลนั้นก่อให้เกิดภาระอย่างมากมายต่อระบบคอมพิวเตอร์ของโจทก์ การกระทำของจำเลยในการปกปิดต้นกำเนิดของอีเมลเหล่านั้นได้กลายเป็นภาระของโจทก์ เพราะโจทก์ถูกบังคับให้ต้องเก็บอีเมลที่ไม่สามารถส่งออกไปได้ โดยไม่สามารถที่จะส่งอีเมลเหล่านั้นคืนกลับไปยังผู้ส่งได้เลย เนื่องจากที่อยู่ที่ปรากฏนั้นไม่มีอยู่จริง ศาลพิเคราะห์แล้วเห็นว่ามูลค่าความเสียหายที่เกิดขึ้นกับการทำให้อุปกรณ์ของโจทก์ด้อยค่าลง แม้ไม่มีความเสียหายจริงๆ กับตัวทรัพย์สินเกิดจากการกระทำของจำเลย นอกจากนี้ CompuServe ยังกล่าวอีกด้วยว่าการเยียวยาที่ดีนั้น ควรจะรวมถึงการเยียวยาความเสียหายอื่นๆ ด้วยเช่น ชื่อเสียงทางธุรกิจ เนื่องจาก CompuServe ได้รับจดหมายต่อว่าจากลูกค้าเฉลี่ยแล้วเป็นจำนวน 50 ฉบับต่อวัน และขู่ว่าจะยกเลิกการเป็นสมาชิก ถ้ายังไม่หยุดส่งอีเมลที่ไม่ได้ร้องขอจำนวนมากดังกล่าว

Cyber Promotions โต้แย้งว่า CompuServe ได้ยินยอมให้บุคคลทั่วไปนั้นใช้เซิร์ฟเวอร์ โดยการยินยอมให้มีการสมัครเพื่อรับอีเมลจากบุคคล หรือใครก็ตาม ไม่ว่าจะให้อยู่แห่งใดบนอินเตอร์เนต ซึ่งเป็นผลให้ Cyber Promotions ได้รับความยินยอมที่จะใช้ทรัพย์สินเหล่านั้นด้วย

อย่างไรก็ตาม ศาลเห็นว่า จำเลยมีส่วนร่วมในช่วงเวลาของการกระทำการส่งข้อมูลอิเล็กทรอนิกส์จำนวนมากในรูปแบบของอีเมลที่ไม่ได้ร้องขอ ไปยังอุปกรณ์คอมพิวเตอร์ที่เป็นทรัพย์สินของโจทก์ จำเลยได้ดำเนินการกระทำเช่นนั้นอย่างต่อเนื่อง หลังจากโจทก์ได้แจ้งแก่จำเลยให้หยุดการกระทำซ้ำๆ เช่นนั้น และจำเลยก็พยายามทุกวิถีทาง ที่จะหลบเลี่ยงความพยายามอย่างมากของโจทก์ ที่จะปกป้องอุปกรณ์คอมพิวเตอร์ของตนจากการถูกลักลอบใช้เช่นนั้น ดังนั้น สิทธิใดๆ ก็ตามที่ได้รับจะสิ้นสุดลงเมื่อ CompuServe ได้แจ้งแก่จำเลยแล้วว่าการเข้าใช้อุปกรณ์ของ CompuServe ไม่เป็นที่ยอมรับได้ โจกท์จึงมีข้อเรียกร้องที่อ้างได้ในเรื่องการละเมิดทรัพย์สินส่วนบุคคล และมีสิทธิที่จะขอให้มีการบรรเทาเบื้องต้นเพื่อที่จะปกป้องทรัพย์สินอื่นๆ ของเขา โดยห้ามจำเลยส่งข้อความโฆษณาใดๆ ไปยังอีเมลแอดเดรสที่ดูแลโดย CompuServe ด้วย

3.4.5.2 เครื่องหมายการค้า (Damage to Trademarks)

นอกเหนือจากประเด็นเรื่องการบุกรุกแล้ว AOL ยังยกเรื่องการหลอกลวงแหล่งกำเนิด (false designation) และความไม่ชัดเจนของเครื่องหมายการค้า (dilution of trademark) ภายใต้ Lanham Act ด้วย ซึ่งตราขึ้นเพื่อให้ความคุ้มครองเครื่องหมายการค้า เพื่อเป็นประกันในชื่อเสียงของเจ้าของในธุรกิจของเขา และคุ้มครองผู้บริโภคในการแยกความแตกต่างระหว่างกันด้วย

การกระทำที่จะถือว่าเป็นการหลอกลวงแหล่งกำเนิด คือ

- ผู้ละเมิดต้องกระทำการต้องการหลอกลวงแหล่งกำเนิด
- ในการหลอกลวงแหล่งกำเนิดนั้นต้องเป็นการหลวงลวงถึงต้นกำเนิด ความเป็นเจ้าของ ความเป็นผู้สนับสนุน
- โจทก์เชื่อว่าเขาเป็นผู้รับความเสียหายจากการกระทำเช่นว่านั้น

ในกรณีนี้ อีเมลที่ส่งนั้นมีข้อความที่เขียนว่า (aol.com) อยู่ในหัวข้อของเมลด้วย ซึ่งเป็นการหลอกลวงถึงแหล่งกำเนิดเมล ทำให้สมาชิกของ AOL เข้าใจผิดว่า AOL เป็นผู้สนับสนุนหรือยอมรับให้มีการส่งสแปมเมลเหล่านั้น*

ศาลเห็นว่าการกระทำดังกล่าวนั้น ก่อให้เกิดความเสียหายจำนวนมากกับ AOL เนื่องจาก AOL นั้นแสดงความเป็นเจ้าอย่างแจ้งชัดในตัวเครื่องหมายการค้า AOL โดยมีการจดทะเบียน และใช้โดย AOL เพื่อให้จดจำได้ในสังคมโลกด้วยสินค้าและบริการ ศาลจึงเห็นว่าเครื่องหมายการค้าถูกทำให้เสื่อมค่าลงโดยผู้ปลอมแปลง

3.4.5.3 Computer Fraud and Abuse Act

AOL ประสบความสำเร็จในการใช้กฎหมายฉบับนี้ต่อด้านสแปมเมล ซึ่งในการใช้สิทธิตามกฎหมายฉบับนี้ โจทก์ต้องพิสูจน์ว่า

- มีการเข้าถึงเครื่องคอมพิวเตอร์ด้วยความตั้งใจ
- การเข้าถึงนั้นเกินขอบอำนาจที่ได้รับ
- การเข้าถึงนั้นทำให้ได้รับข้อมูลบางอย่าง
- คอมพิวเตอร์นั้นได้รับการปกป้อง
- การกระทำนั้นเกี่ยวข้องกับการสื่อสารระหว่างกัน

ซึ่ง AOL ก็แสดงให้เห็นว่า NHCD นั้นได้ทำการรวบรวม (harvesting) ข้อมูลอีเมลของ สมาชิก AOL และทำการส่งเมลจำนวนมากโดยไม่ได้รับอนุญาต เข้ามาในระบบคอมพิวเตอร์ของ AOL

เป็นการยากที่จะทำนายถึงผลกระทบในท้ายที่สุดของ CAN SPAM แต่มีความเป็นไปได้ที่จะทำนายถึงขอบเขตของสแปมในอนาคต ตราบเท่าที่ยังมีการทำเงินได้จากสแปม สแปมก็

---

* ดูภาคผนวก ข.

ยังคงเป็นส่วนหนึ่งในชีวิตประจำวันของเราไปเรื่อยๆ แม้ว่าสแปมเมอร์จะถูกบังคับให้จัดการกับสภาพแวดล้อมของความโกรธแค้นที่เพิ่มขึ้นเรื่อยๆ

3.4.6 ประสิทธิภาพและปัญหาที่เกิดขึ้นจากการบังคับใช้ CAN SPAM Act of 2003

นับตั้งแต่กฎหมายฉบับนี้มีผลบังคับใช้เมื่อวันที่ 1 มกราคม 2004 เป็นต้นมา คณะกรรมการ FTC ได้นำคดีที่ถูกกล่าวหาว่าละเมิดบทบัญญัติตามกฎหมายฉบับนี้ขึ้นสู่ศาลแล้วไม่ต่ำกว่า 20 คดี ในขณะที่ DOJ, อัยการรัฐ และผู้ให้บริการอินเตอร์เนต ได้ฟ้องคดีต่อศาลรัฐบาลกลางเพิ่มเติมไม่น้อยกว่า 30 คดี เพื่อบังคับตามกฎหมายนี้

ทั้งนี้ จากรายงานของ FTC[36] ที่ต้องนำส่งต่อสภาคองเกรซตามเงื่อนไขใน CAN SPAM จากประสบการณ์การบังคับใช้กฎหมายของ FTC และหน่วยงานที่มีอำนาจบังคับใช้กฎหมายที่เกี่ยวข้องนั้น มีความเห็นว่า การบังคับใช้กฎหมายฉบับนี้ ประสบผลสำเร็จตามเป้าหมายที่ตั้งไว้สองประการคือ

หนึ่ง เงื่อนไขที่สำคัญตามกฎหมายนั้น ที่มุ่งหมายให้มีอีเมลเชิงพาณิชย์ที่กระทำการอย่างตรงไปตรงมาเพิ่มขึ้น ได้รับการปฏิบัติตามโดยนักการตลาดออนไลน์ที่ถูกกฎหมายจำนวนมาก และสอง คือ กฎหมายนี้ ได้ให้อำนาจหน่วยงานในการบังคับใช้กฎหมายของรัฐ และ ISPs ด้วยเครื่องมือที่เพิ่มมากขึ้นในการนำคดีขึ้นสู่ศาล ซึ่งก็ปรากฏว่ามีมากกว่า 50 คดีถูกดำเนินการโดยหน่วยงานเหล่านี้อย่างมีประสิทธิภาพ

ความคาดหวังบางอย่างต่อปัญหาสแปม เช่นมิติในทางระหว่างประเทศ อาจไม่เปลี่ยนแปลงไปในสาระสำคัญเนื่องจากการตรากฎหมาย CAN SPAM แต่ในหลายๆ ทางภาพรวมเกี่ยวกับอีเมลนั้นมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ และส่วนมากเป็นไปในทางที่ดีขึ้น จำนวนสแปมเมลที่ส่งไปทั่วอินเตอร์เนตไม่มีการเพิ่มขึ้นแต่อย่างใด และจำนวนอีเมลที่เข้าถึงกล่องจดหมายของผู้บริโภคทั้งหลายก็มีจำนวนที่ลดลงด้วย แม้ว่าส่วนมากจะเกิดจากเทคโนโลยีการต่อต้านสแปมเมลที่มีประสิทธิภาพมากขึ้นด้วยก็ตาม นอกจากนี้ยังมีอัตราการลดลงของจำนวนสแปมที่มีเนื้อหาเกี่ยวกับเรื่องเพศ ส่วนนักการตลาดออนไลน์ที่ถูกกฎหมายก็ปรับใช้ CAN-SPAM กันจำนวนมาก ปรากฏการณ์ที่เกิดขึ้นพร้อมกันเช่นนี้ ทำให้ผู้บริโภคเริ่มที่จะรายงานถึงความรบกวนของสแปมเมลเข้ามาลดลง การ

---

[36] Federal Trade Commission, "Effectiveness and Enforcement of the CAN-SPAM Act : A Report to Congress," at i-iii (December 2005), available at http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

พัฒนาการเหล่านี้ชี้ให้เห็นว่าสแปมไม่ใช่สิ่งที่น่ากลัว และทำลายซึ่งความน่าเชื่อถือของอีเมล อย่างที่เคยเกิดขึ้นในอดีต

อย่างไรก็ตาม ความเปลี่ยนแปลงบางอย่างที่เกิดขึ้น เนื่องจากการปรับใช้กฎหมายฉบับนี้ก็ก่อให้เกิดปัญหาด้วยเช่นกัน ตัวอย่างเช่น การเปลี่ยนไปของเนื้อหาสแปมเมลที่มีจุดมุ่งหมายที่ไม่ดีเพิ่มมากขึ้น และจำนวนมากกว่าสแปมที่เป็นอีเมลที่โฆษณาสินค้า และบริการที่แท้จริง สแปมเมลจำนวนมากปัจจุบันนี้ได้รวมเอารูปแบบที่เรียกว่า "malware" ที่เป็นอันตรายต่อผู้รับ ซึ่งแทนที่จะแก้ไขเนื้อหาในสแปมเมลของพวกเขา สแปมเมอร์กลับค้นหาวิธีที่ที่จะทำให้การบังคับใช้กฎหมายอ่อนแอลงโดยการใช้การจัดการทางธุรกิจที่มีความสลับซับซ้อนให้มากยิ่งขึ้น ยิ่งไปกว่านั้น สแปมเมอร์ยังคงปกปิดตัวตนที่แท้จริงของตัวเอง โดยการใช้ข้อมูลที่ผิดๆ ต่อนายทะเบียนชื่อโดเมน ข้อมูลที่ไม่ถูกต้องที่พอประเมินค่าได้ในฐานข้อมูลของนายทะเบียน และความล้มเหลวของนายทะเบียนในการหามาตรการที่เหมาะสมเพื่อที่จะยืนยันถึงความถูกต้องที่แท้จริงของข้อมูลเก็บรวบรวมไว้โดยนายทะเบียนนั้น เป็นอันตรายต่อการบังคับใช้กฎหมายอย่างต่อเนื่อง

ทั้งนี้ คณะกรรมการ FTC ได้นำเสนอมาตรการที่จะปรับปรุงให้การบังคับใช้ CAN-SPAM ACT มีประสิทธิภาพมากยิ่งขึ้น โดยประการแรกนั้น ขณะที่ยังไม่มีการแนะนำให้แก้ไข CAN-SPAM ACT เพิ่มเติม FTC อยากให้สภาคองเกรซเร่งผ่านกฎหมายที่ชื่อว่า US SAFE WEB ACT ซึ่งจะพัฒนาความสามารถของ FTC อย่างมากต่อการบังคับใช้ CAN-SPAM ACT เพื่อติดตามสแปมเมอร์ และผู้ขายที่ดำเนินการภายนอกเขตแดนของสหรัฐฯ ร่วมกับความพยายามด้านการศึกษา และการบังคับใช้การบังคับใช้ในระหว่างประเทศอย่างไม่หยุดยั้ง สิ่งนี้จะช่วยพัฒนาความสามารถในการบังคับใช้กฎหมายเพื่อจัดการกับปัญหาอันเป็นความท้าทายที่เกิดขึ้นจากสแปมเมลที่มาจากต่างประเทศโดยธรรมชาติ

ประการที่สอง ความพยายามในการให้ความรู้อย่างต่อเนื่องเป็นสิ่งที่จำเป็น เพื่อที่จะให้แน่ใจได้ว่าผู้บริโภคนั้นตระหนักถึงวิธีการที่หลากหลาย ซึ่งพวกเขา และลูกหลาน สามารถป้องกันตนเองจากการได้รับ และการเข้าถึงสแปมเมลที่เกี่ยวกับเรื่องเพศ เครื่องมือที่สามารถหาได้จาก ISPs และโปรแกรมที่สามารถหาซื้อได้ รวมถึงการปกป้องที่เกิดขึ้นโดยกฎหมาย สามารถลดโอกาส ที่ผู้บริโภค โดยเฉพาะลูกหลานของพวกเขา จะถูกโจมตีจากการแจกจ่ายภาพลามกโดยผ่านสแปม

ประการที่สาม คณะกรรมการเห็นควรให้มีการเร่งพัฒนาเทคโนโลยีในการต่อต้านสแปม และโดยเฉพาะถึงความน่าเชื่อถือในระดับโดเมนเนม เทคโนโลยีนี้ ผนวกกับระบบที่มีชื่อเสียง

และเชื่อถือได้ สร้างความหวังอันยิ่งใหญ่ในการทำให้แน่ใจว่า สแปมเมอร์จะไม่สามารถที่จะใช้วิธีการโดยปกปิดตัวตนที่แท้จริงต่อไปได้

## 3.5 แนวคิดทางกฎหมายและมาตรการทางกฎหมายกับจัดการกับปัญหาจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์ในสหภาพยุโรป

### 3.5.1 ความเป็นมาของ Directive on Privacy and Electronic Communications

ในสหภาพยุโรป หรือ EU และสมาคมเขตการค้าเสรี หรือ EFTA สนับสนุนการต่อต้านสแปมเมล ทั้งนี้เห็นได้จาก Directive 2002/58/EC of the EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications) ออกมาในเดือนกรกฎาคม 2002 เพื่อให้เป็นเค้าโครงด้านกฎหมายที่เกี่ยวกับการสื่อสารทางอิเลคทรอนิคส์ทั้งหมด ในเรื่องของข้อมูลส่วนบุคคล (Personal Data) และการคุ้มครองความเป็นส่วนตัวจากการสื่อสารผ่านทางอิเลคทรอนิคส์ ซึ่งไม่จำกัดเพียงแค่อินเตอร์เนตและคอมพิวเตอร์เท่านั้น ซึ่ง Directive ฉบับนี้นั้นเป็นผลมาจาก 1999 Telecommunications Review ที่มองหาแนวทางทั้งหมดของนโยบาย ที่เกี่ยวข้องการการสื่อสารในสหภาพยุโรป

ทั้งนี้ ด้วยเหตุผลที่ว่า จาก article 12 ของ Directive 97/66/EC ซึ่งให้การคุ้มครองการติดต่อโดยไม่ได้รับอนุญาตเพื่อทำการตลาดแบบตรง โดยในบริบทของคำว่า "call" นั้น อาจถูกตีความอย่างแคบได้ โดยการออกกฎหมายที่คุ้มครองเพียงการตลาดทางโทรศัพท์ โดยไม่รวมถึงอีเมล และการสื่อสารในรูปแบบอื่นๆ ดังนั้น เพื่อให้สามารถครอบคลุมเทคโนโลยีดังกล่าวได้ คำว่า "call" จึงถูกใช้ในรูปของ "communication" แทน ยิ่งไปกว่านั้น การใช้อีเมลเพื่อวัตถุประสงค์ในการทำการตลาดแบบตรง นอกจากการร้องขอจากผู้บอกรับเป็นสมาชิกแล้ว ควรจะได้รับการคุ้มครองเช่นเดียวกับการสื่อสารโดยวิธีอื่นๆ ซึ่งหมายความห้ามส่งสแปมนอกจากว่าจะได้รับอนุญาตจากผู้ที่ตอบรับว่าต้องการที่จะได้รับเมลเพื่อการตลาดแบบตรงเหล่านั้น

ประเทศสมาชิกของสหภาพยุโรปที่ได้ตรากฎหมายโดยใช้รูปแบบวิธี Opt-in นั้น ได้แก่ ออสเตรีย, เดนมาร์ก, ฟินแลนด์, เยอรมัน, กรีซ และอิตาลี ส่วนกลุ่มประเทศที่รับเอาวิธี Opt-out นั้นได้แก่ ประเทศเบลเยี่ยม และสเปน

นอกจากนี้กฎหมายอีกหลายฉบับ ที่มีบทบัญญัติต่อต้านสแปมที่คล้ายคลึงกับบทบัญญัติหลักใน E-Privacy Directive ก็สามารถถูกพบได้อย่างกระจัดกระจายใน Directive ฉบับก่อนๆ ที่ออกกฎเรื่องการพาณิชย์อิเล็กทรอนิกส์อย่างทั่วไป และสามารถนำมาปรับใช้กับกรณีของสแปมเมลได้คือ

- E-Privacy Directive 2002/58/EC
- E-Commerce Directive 2000/31/EC
- Telecommunications Privacy Directive 97/66/EC
- Distance Contract Directive 97/7/EC
- Data Protection Directive 95/46/EC

3.5.2 มาตรการที่นำมาใช้ใน Directive on Privacy and Electronic Communications

Article 13 - Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than

those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

โดยหลักการของ Directive ห้ามการส่งเอกสารใดๆ ในเชิงพาณิชย์ไม่ว่าจะเป็น อีเมล แฟกซ์ หรือเครื่องตอบรับอัตโนมัติอื่นๆ โดยปราศจากคำอนุญาตยินยอมของผู้ใช้ วิธีการทำการตลาดโดยตรงสามารถทำได้ เฉพาะในกรณีที่ได้รับความยินยอมจากผู้มีสิทธิให้ความยินยอมเท่านั้น หรือที่เรียกว่า ระบบ Opt-in ในการส่งอีเมลเชิงพาณิชย์ทั้งหมดถึงผู้รับแต่ละราย (Individual Subscribers) ซึ่งหมายความธุรกิจใดๆ ในกลุ่มยุโรปสามารถที่จะส่งอีเมลถึงผู้รับแต่ละรายได้เมื่อได้รับความยินยอมโดยตรงเท่านั้น

ข้อยกเว้นในเรื่องการให้ความยินยอมของมาตรการ Opt-in คือในกรณีที่ยังคงมีการติดต่อสัมพันธ์กับลูกค้าอยู่นั้น การส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอสามารถกระทำได้ จนกว่าจะมีการร้องขอจากผู้รับให้ยุติการสื่อสารเช่นว่านั้น

เงื่อนไขที่สำคัญประการหนึ่งภายใต้ข้อยกเว้นอันนี้คือ ธุรกิจนั้น ต้องได้รับที่อยู่อีเมลของลูกค้าในระหว่างช่วงระยะเวลาของการขาย หรือการตกลงเจรจาซื้อขายสินค้า หรือบริการ และต้องเป็นการทำการตลาดต่อเนื่องในสินค้า และบริการที่คล้ายคลึงกันในธุรกิจนั้น โดยต้องได้รับที่อยู่มาโดยสุจริต ในขอบเขตของการปกป้องข้อมูลที่มีอยู่ และต้องจัดให้มีมาตรการ Opt-out คือมีสิทธิที่จะบอกเลิกการรับข้อมูลข่าวสารเมื่อใดก็ได้เสมอโดยไม่เสียค่าใช้จ่ายใดๆ

กฎหมายยังกำหนดให้ผู้ส่งอีเมลเชิงพาณิชย์ไม่ปกปิดตัวตนที่แท้จริงของตนเอง และจัดให้มีที่อยู่กลับที่สมบูรณ์ที่ผู้รับจะสามารถส่งคำร้องขอไม่รับข่าวสารได้ ซึ่งเงื่อนไขนี้มีเป้าหมายเพื่อต่อสู้กับการกระทำที่หลอกลวง และใช้ที่อยู่อีเมลที่ไม่เป็นจริง

เป็นที่น่าสังเกตว่า บทบัญญัติของสหภาพยุโรปนี้ครอบคลุมการส่งอีเมลถึงผู้ใช้อีเมลส่วนบุคคลเท่านั้น ไม่นำมาใช้ในการสื่อสารระหว่างธุรกิจถึงธุรกิจ ซึ่งทำให้เกิดความรู้สึกว่าน่าจะเป็นการละเมิดความสัมพันธ์ทางธุรกิจ

มีจำนวนประเทศสมาชิกที่ได้ออกกฎหมาย ห้ามการส่งอีเมลเพื่อการพาณิชย์โดยไม่ได้รับอนุญาตเรียบร้อยแล้ว ส่วนสมาชิกประเทศอื่นก็ได้รับเอาไปออกกฎหมายภายในของตนเช่นกัน ในขณะที่ประเทศสมาชิกส่วนใหญ่มักจะใช้มาตรการ Opt-out ซึ่งจากมุมมองของนักการตลาดภายในประเทศ วิธีนี้ไม่เป็นที่น่าพอใจนัก นักการตลาดแบบตรงในประเทศที่ใช้ระบบ Opt-in อาจจะไม่จัดกลุ่มเป้าหมายโดยอีเมลที่อยู่ภายในประเทศของพวกเขา แต่พวกเขาจะส่งสแปมเมลออกไปยังประเทศที่ใช้ระบบ Opt-out แทน ยิ่งไปกว่านั้น อีเมลแอดเดรสของแต่ละคนยังไม่สามารถที่จะบ่งชี้ถึงที่อยู่อาศัยของผู้รับได้ ดังนั้นระบบกฎหมายที่แตกต่างซึ่งอยู่ในตลาดเดียวกันอาจจะใช้ไม่ได้ในทางปฏิบัติ ดังนั้นแนวทางปฏิบัติที่เป็นไปในแนวทางเดียวกันน่าจะเป็นผลดีกว่าในการแก้ไขปัญหานี้

3.5.3 ความคาดหวังต่อความมีประสิทธิภาพของ Directive on Privacy and Electronic Communications[37]

สแปมไม่ได้ถูกจำกัดความหรือถูกอ้างถึงอย่างเฉพาะเจาะจงใน the European Union Directive 2002/58/EC on Privacy and Electronic Communications ใน Directive ใช้คำว่า "unsolicited communications" by "electronic mail" "for the purposes of direct marketing" ซึ่งก็มีความแตกต่างกับคำนิยามสแปมเมลของสหรัฐฯ ซึ่งใช้คำว่า "unsolicited commercial electronic mail" ดังที่ได้กล่าวมาแล้ว

ความแตกต่างในเรื่องคำนิยามนี้ อาจจะก่อให้เกิดวิกฤติเรื่องคำจำกัดความได้ในทางพิจารณาคดี เช่น อังกฤษในลักษณะเฉพาะ และอียูโดยทั่วไป ที่กฎหมายสแปมรับเอาวิธี "opt-in" เป็น

---

[37] Reagan Smith, "Eliminating The Spam From Your Internet : the possible effects of the unsolicited commercial electronic mail act of 2001 on junk e-mail," Texas Tech Law Review 35, 411 (2004) : 11.

นโยบายพื้นฐานในเรื่องการให้ความยินยอมต่อการส่งสแปม ตัวอย่างหนึ่งในหลายๆ ตัวอย่างเช่น Regulation 22(2) of the United Kingdom Privacy and Electronic Communications (EC Directive) Regulations จัดให้การส่งสแปมเมลผ่านการสื่อสารที่ไม่ได้ร้องขอ เพื่อวัตถุประสงค์ของการตลาดขายตรงไม่สามารถทำได้ ถ้าปราศจากความยินยอมมาก่อนแล้วของผู้รับ ซึ่งเป็นวิธีการให้ความยินยอมแบบ "opt-in" ในการส่งสแปม ซึ่งก่อให้เกิดประเด็นที่เกี่ยวข้องว่าเมื่อไรสแปมจึงจะกลายเป็นสแปม ตัวอย่างเช่น ถ้ามีการให้ความยินยอมมาก่อน การสื่อสารที่ไม่ได้ร้องขอที่ส่งตามมาหลังจากความยินยอมเช่นนั้นน่าจะมีฉันทามติโดยเด็ดขาดว่าไม่นับจำนวนว่าเป็นสแปม ในระหว่างช่วงเวลาที่ไม่มีหลักฐานว่ายืนยันการถอนการให้ความยินยอม หรือลบล้างความยินยอมของผู้รับ

เงื่อนไขหลักประการแรกของ E-Privacy Directive[38] คือการต้องการให้มีการยินยอมก่อนของสมาชิกก่อนการส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอสำหรับการตลาดโดยตรง ซึ่งเป็นที่ทราบกันดีอีกนัยหนึ่งว่าการควบคุมการส่งอีเมลบนพื้นฐานของการให้ความยินยอมแบบ "opt-in" ซึ่งแตกต่างจากวิธีที่ไม่ต้องได้รับความยินยอมอย่าง "opt-out" ใน CAN SPAM Act เนื่องจากในการเจรจาต่อรองของ the E-Privacy Directive ที่ Luxembourg ได้คัดค้านกลยุทธ์ "opt-in" บนหลักการที่ว่ามันเป็น "การไม่เหมาะสม", "ไม่มีความสมดุล", และ "ไร้จุดยืน" แต่กระนั้นก็ดี ประเทศสมาชิกส่วนมากได้สนับสนุนนโยบาย "opt-in" และเงื่อนไขใน the E-Privacy Directive

เหตุผลอันสมควรสำหรับนโยบาย "opt-in" คือเพื่อป้องกันความเป็นส่วนตัวของสมาชิกอินเตอร์เนต ซึ่งเป็นนโยบายหลักของการจัดการทางพาณิชย์อิเล็กทรอนิกส์ของกลุ่มยุโรป อย่างไรก็ตาม นโยบาย "opt-in" จะสามารถรอดพ้นจาก European Court of Justice (ECJ) หรือไม่ ก็น่าจะขึ้นอยู่กับความสม่ำเสมอว่าศาลเข้าใจมันในฐานะข้อจำกัดของกฎในการโฆษณาหรือไม่ ในคดี KO v. Gourmet International Products AB ศาล ECJ ถือว่าการห้ามการโฆษณาโดยตรงทั้งหมดไปยังผู้บริโภค (เช่นการโฆษณาในหนังสือพิมพ์ บนวิทยุ และบนโทรทัศน์ ส่งวัตถุที่ไม่ได้ร้องขอไปโดยตรง หรือการแปะโปสเตอร์บนไฮเวย์สาธารณะ) ในเครื่องดื่มแอลกอฮอล์ (โดยการแสดงถึง) การบริโภคซึ่งเชื่อมโยงกับการกระทำทางสังคมที่เป็นประเพณี และที่เป็นนิสัยของท้องถิ่น และธรรมเนียมเป็นความรับผิดที่ขัดขวางการเข้าถึงตลาดโดยผลิตภัณฑ์จากรัฐสมาชิกอื่นๆ มากกว่ามันขัดขวางการเข้าถึงโดยผลิตภัณฑ์ภายในประเทศ ที่ซึ่งผู้บริโภคมีความคุ้นเคยมากกว่าในไม่ช้า ศาลกล่าวเพิ่มเติมว่าอย่างไรก็ดี, ข้อจำกัดเช่นนั้นสามารถที่จะถูกสนับสนุนบนพื้นฐานของการปกป้องสุขภาพของสาธารณะ

---

[38] Taiwo A. Oriola, p.13.

ซึ่งอาจถูกมองได้ว่าศาลยุโรปจะสนับสนุนนโยบายสแปม "opt-in" บนพื้นฐานของความเป็นส่วนตัวหรือไม่ ในการเผชิญหน้ากับความท้าทายต่อข้อจำกัดในการโฆษณาที่อาจเป็นไปได้ หรือมันน่าจะถูกเข้าใจว่าเป็นการจำกัดการโฆษณาในบริบทของคำตัดสินของ ECJ ในคดี Gourmet International Products AB หรือไม่ เนื่องจากความเป็นไปได้ในการกีดขวางการเข้าถึงผู้บริโภคที่มีศักยภาพต่อสินค้าและบริการของผู้โฆษณาในประเทศสมาชิก หรือมันน่าจะถูกเข้าใจว่าเป็นข้อจำกัดที่ถูกกฎหมาย ซึ่งเป็นสิ่งที่สมควรอย่างยิ่ง บนพื้นฐานของความเคารพซึ่งความเป็นส่วนตัว

เงื่อนไขหลักประการที่สองของ E-Privacy Directive คือยอมให้ธุรกิจทั้งหลายที่จะใช้รายละเอียดการติดต่อทางอิเล็กทรอนิกส์ของลูกค้า ที่ได้มาโดยวิธีการติดต่อทางการค้าระหว่างกันเพื่อผลทางการตลาดโดยตรงซึ่งสินค้าและบริการที่คล้ายคลึงกันในอนาคต อย่างไรก็ตาม ลูกค้าต้องได้รับโอกาสที่จะปฏิเสธการใช้รายละเอียดการติดต่อทางอิเล็กทรอนิกส์ของพวกเขาเช่นนั้นโดยไม่มีค่าใช้จ่าย เงื่อนไขนี้ไม่ได้ทำให้เสียไปซึ่งนโยบาย "opt-in" เนื่องจากการให้ความยินยอมก่อนของลูกค้าก็เป็นสิ่งสำคัญต่อการส่งเสริมการนำข้อมูลไปใช้เช่นนั้น ดูเหมือนว่าจะเป็นความยากลำบากของ E-Privacy Directive ที่จะรักษาไว้ซึ่งความสมดุลที่เท่ากันระหว่าง สิทธิส่วนตัวของลูกค้า และการโฆษณาทางธุรกิจที่ถูกกฎหมาย ซึ่งเป็นความท้าทายอันยิ่งใหญ่ต่อแนวทางทั้งหมดของมาตรการการต่อต้านสแปม

เงื่อนไขสำคัญที่สามของ E-Privacy Directive คือ ข้อห้ามของมันในการปลอมแปลงหรือปกปิดซึ่งตัวตนของผู้ส่งข้อความอีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอ หรือการส่งอีเมลที่ไม่ได้ร้องขอโดยปราศจากที่อยู่กลับของอีเมลของผู้ส่งที่สมบูรณ์ เพื่อจุดประสงค์ของการตลาดโดยตรง ซึ่งเป็นเรื่องเดียวกันกับบทบัญญัติการให้มีหัวเรื่องอีเมลที่แท้จริง และการให้มีฉลากในมาตรา 5 ของ CAN-SPAM Act ของสหรัฐฯ และสามารถก่อให้เกิดประเด็นที่คล้ายคลึงกันเรื่องการพูดอย่างอิสระ และการไม่เปิดเผยตัวตนในยุโรปได้

ยูโรปนั้นเป็นที่ทราบกันมายาวนานว่า มีความโน้มเอียงสูงของอี-คอมเมิร์ซ ต่อการบุกรุกทั้งโดยตรง หรือโดยอ้อมต่อความเป็นส่วนตัว โดยเฉพาะในบทบัญญัติข้อ 8(1) และ (2) ใน the European Convention on Human Rights ซึ่งรับรองสิทธิในความเป็นส่วนตัวและชีวิตครอบครัว ตามที่ Henrik W.K. Kaspersen เคารพว่าชีวิตส่วนตัวได้รับการยอมรับในฐานะสิทธิมนุษยชนจากจำนวนคำตัดสินของศาลสิทธิมนุษยชนของยุโรป (European Court of Human Rights) ใน Strasbourg ตัวอย่างเช่น ในคดี Perry v. United Kingdom, ศาลสิทธิมนุษยชนของยุโรป นิยามคำว่า "private life" อย่างกว้างๆ ดังต่อไปนี้

"private life" เป็นคำที่กว้างมาก และข้อเกี่ยวกับหลักเกณฑ์หลายประการ เช่น การแยกแยะเพศ, ชื่อ, คำแนะนำเกี่ยวกับเพศ และชีวิตทางเพศ จึงเป็นพื้นฐานที่สำคัญต่อขอบเขตส่วนบุคคลที่ได้รับการปกป้องโดยบทบัญญัติข้อ 8 ซึ่งปกป้องสิทธิที่จะแสดงตัวและการพัฒนาตัวเอง และสิทธิที่จะสร้างและพัฒนาความสัมพันธ์กับมนุษย์คนอื่นๆ และนอกโลก และมันอาจจะรวมถึงกิจกรรมโดยธรรมดาทางธุรกิจ หรือเกี่ยวกับวิชาชีพ ดังนั้น มีขอบเขตความสัมพันธ์ของบุคคลกับคนอื่นๆ หรือแม้แต่ในทางสาธารณะ ซึ่งอาจจะตกอยู่ภายในขอบเขตของ "private life"

ดังนั้น จึงเป็นสิ่งที่น่าสนใจที่จะทราบว่าศาลแห่งชาติ และศาลสิทธิมนุษยชนของยุโรปน่าจะตีความเงื่อนไขการให้มีหัวเรื่องอีเมลที่แท้จริงของ E-Privacy Directive ในทางใด ศาลในยุโรปจะให้เหตุผลสนับสนุนเงื่อนไขการมีฉลากและการมีหัวเรื่องอีเมลที่แท้จริง ซึ่งไม่อาจหลีกเลี่ยงต่อความเคารพในความเป็นส่วนตัวและชีวิตครอบครัว ตามที่ได้รับการรับรองโดยบทบัญญัติข้อ 8 ของ the European Convention on Human Rights หรือไม่ และศาลถือหรือไม่ว่าเงื่อนไขเป็นข้อจำกัดแต่แรกซึ่งการพูดโดยอิสระ ดังนั้นละเมิดบทบัญญัติข้อ 10 ของ the European Convention on Human Rights ในคดี Gaweda v. Poland ศาลสิทธิมนุษยชนของยุโรป ขณะที่ตีความมาตรา 10 ของ the Human Rights Convention เรื่องเสรีภาพในการแสดงออก ให้ความเห็นว่า

ภายใต้บทบัญญัติข้อ 10(2) เสรีภาพในการแสดงออกที่สามารถนำมาประยุกต์ ไม่เพียงแต่เป็น "ข้อมูล" หรือ "ความคิด" ที่ได้รับการยอมรับอย่างเต็มใจ หรือในเรื่องที่ไม่ผิดกฎหมาย หรืออะไรก็ตามที่ไม่แตกต่างเท่านั้น แต่ "ข้อมูล" หรือ "ความคิด" ยังรวมถึงสิ่งที่ผิดกฎหมาย, ทำให้ตกตะลึงหรือรบกวนด้วยเช่นกัน เหล่านั้นเป็นไปตามความต้องการของเสียงส่วนมาก, ความอนทน และการมีจิตใจกว้างขวางโดยปราศจากซึ่งการไม่มี "สังคมประชาธิปไตย"

ความท้าทายที่ยิ่งใหญ่ที่สุดของศาลยุโรปในขณะนี้คือ การที่จะรักษาไว้ซึ่งความสมดุลระหว่างการชิงชัยกันของสิทธิในการพูดอย่างอิสระ และความเป็นส่วนตัว ชะตาของบทบัญญัติ 13(4) of the E-Privacy Directive ต่อการมีหัวเรื่องอีเมล และการมีฉลากที่แท้จริงของข้อความอิเล็กทรอนิกส์ที่ไม่ได้ร้องขอเพื่อวัตถุประสงค์ทางการตลาดโดยตรง น่าจะขึ้นอยู่กับว่าความสมดุลเอียงไปทางใด

โดยนัย, article 15(2) of the E-Privacy Directive เข้ากันกับ มาตรา 22 ของ Data Protection Directive ซึ่งยอมให้ปัจเจกชนในประเทศสมาชิกฟ้องคดีสำหรับข้อกล่าวหาว่าละเมิดเงื่อนไขใดๆ ของกฎหมายการต่อต้านสแปมของชาติ ซึ่งเป็นความแตกต่างอย่างเห็นได้ชัดจาก CAN

SPAM Act ที่ไม่มีสิทธิตามกฎหมายโดยตรงที่จะฟ้องคดีแพ่งสำหรับการละเมิดบทบัญญัติของกฎหมายข้อใดๆ ที่ถูกกล่าวหา อย่างไรก็ตาม ยังคงที่จะพบเห็นได้ว่าทั้งสมาชิกในสหรัฐฯ หรือผู้รับข้อความอิเล็กทรอนิกส์ที่ไม่ได้ร้องขอ (นอกจาก ISPs) สามารถอาศัยข้อได้เปรียบของคำตัดสินของสหรัฐในคดี Compuserve ที่จะสนับสนุนข้อเรียกร้องทางกฎหมายเรื่องการละเมิดสังหาฯ ได้ และโดยอาศัยบทบัญญัติ 15(3) ของ the E-Privacy Directive ร่วมกับบทบัญญัติ30(1)(c) ของ the Data Protection Directive ได้

3.5.4 ความมีประสิทธิภาพ และการบังคับใช้ E-Privacy Directive ในกลุ่มประเทศ

ใน E-Commerce Directive (2000/31/EC) กฎของประเทศผู้รับ (country of reception) จะถูกนำมาใช้ก่อนสำหรับการสื่อสารเชิงพาณิชย์ที่ไม่ได้ร้องขอ แต่ในทางตรงกันข้ามกับ Directive ที่เหลือซึ่งสนับสนุนหลักการของประเทศต้นกำเนิด (country of origin) ในทางพาณิชย์อิเล็กทรอนิกส์มากกว่า อันเป็นผลให้ ทุกบริษัทในกลุ่มยุโรปต้องเชื่อถือในกฎของสมาชิกกลุ่มสหภาพยุโรปที่อีเมลเชิงพาณิชย์ที่ไม่ได้ร้องขอของพวกเขาอาจจะได้รับที่ใดก็ได้ ทั้งนี้ ประเทศสมาชิกทั้งหมดต้องมีการออกกฎหมายภายในตามแนวทางของ E-Privacy Directive ภายใน 31 ตุลาคม 2003 ที่ผ่านมา ซึ่งแต่ละประเทศก็ได้ออกมาตรการภายในประเทศตนเอง ตามแนวทางของ E-Privacy Directive แล้ว

## 3.6 แนวคิดทางกฎหมายและมาตรการทางกฎหมายกับจัดการกับปัญหาจดหมายอิเล็คทรอนิคส์ที่ผู้รับไม่พึงปรารถนาในเกาหลีใต้

เกาหลีใต้เป็นประเทศที่มีอัตราในการส่งสแปมเมลออกไปทั่วโลกสูงที่สุดในเอเชีย เนื่องจากการการตื่นตัว และการเริ่มมีมาตรการทางกฎหมายในการต่อต้านสแปมของรัฐต่างๆ ในสหรัฐฯ และประเทศในกลุ่มสหภาพยุโรป จึงทำให้สแปมเมอร์ส่วนใหญ่ต้องย้ายฐานการส่งสแปมเมลที่อยู่ในสหรัฐฯ ออกไปนอกประเทศ เพื่อหลีกเลี่ยงกฎหมายที่รุนแรงในสหรัฐฯ ประเทศในเอเชียจึงกลายเป็นกลุ่มเป้าหมายขนาดใหญ่ในการแจกจ่ายสแปมเมลไปยังทั่วโลก โดยเฉพาะประเทศที่มีการพัฒนาทางเทคโนโลยีการสื่อสารสูงอย่างเกาหลี และญี่ปุ่น เพราะยังไม่มีมาตรการทางกฎหมายที่เข้มแข็งพอ เกาหลีใต้จึงประสบปัญหาไม่น้อยจากการหลั่งไหลเข้ามาอย่างมากมายของสแปมเมล โดยในปี 2003 ผู้ใช้อีเมลมีอัตราการได้รับสแปมเมลโดยเฉลี่ยต่อวันเพิ่มขึ้นเป็น 50 ฉบับต่อวัน ซึ่งเป็นอัตราการเพิ่มขึ้นที่สูงมากเมื่อเปรียบเทียบกับอัตราเฉลี่ยในปี 2001 คือ 4.7 ฉบับต่อวัน ทั้งนี้ ยังไม่นับรวมถึงรายงานและคดีต่างๆ ในเรื่องสแปมเมลต่างๆ ที่เข้ามาสู่ศาลจำนวนมาก โดยส่วนใหญ่แล้ว ปัญหาของส

แปมเมลที่พบส่วนใหญ่มักเป็นเรื่องเนื้อหาที่ผิดกฎหมาย และมีลักษณะที่เป็นอันตราย ต่อผู้รับที่เป็นเยาวชน

เกาหลีใต้นั้นไม่มีกฎหมายเฉพาะในเรื่องที่เกี่ยวกับสแปม แต่มีกฎหมายหลายฉบับที่ได้รวมมาตรการในการต่อต้านสแปมเมลไว้บางส่วน และต้องการให้มีมาตรการที่เรียกว่า Opt-out ซึ่งกฎหมายเหล่านั้นได้แก่ The Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 ตามกฎหมายฉบับนี้ สแปม หมายถึง ข้อมูลเชิงพาณิชย์ใดๆ ที่ส่งผ่านอีเมล โทรศัพท์ เครื่องแฟกซ์ และอื่นๆ ที่ส่งถึงผู้รับที่ให้การปฏิเสธไว้โดยชัดแจ้ง โดยกฎหมายห้ามบุคคลใดส่งโฆษณา เพื่อวัตถุประสงค์ในทางธุรกิจที่ร้องขอไปยังผู้รับที่ได้ให้การปฏิเสธการรับข้อมูลเช่นนั้นอย่างชัดเจนไว้แล้ว กฎหมายยังต้องการให้ผู้ส่งแสดงวัตถุประสงค์ของข้อความเช่นนั้นโดยชัดแจ้ง อันได้แก่ เนื้อหาโดยหลัก, ชื่อของผู้ส่ง, วิธีการติดต่อ และวิธีใช้ของผู้รับในการที่จะปฏิเสธการรับข้อความโฆษณาเช่นนั้นในอนาคตอย่างไร

คณะกรรมการการค้าเสรีของเกาหลี หรือ Korea Fair Trade Commission (KFTC) ซึ่งเป็นคณะกรรมการที่ตั้งขึ้นเพื่อมากำกับดูแลปัญหาที่เกิดจากการสแปมเมล และมีการปรับปรุงกฎหมายที่เกี่ยวข้องกับสแปมเมล โดยเพิ่มมาตรการการลงโทษให้มากขึ้นเพื่อจัดการกับผู้ที่ส่งสแปมเมลที่มีเนื้อหาที่ไม่เหมาะสมกับเยาวชน และจัดให้มีระบบด้วยวิธีซึ่งผู้บริโภคสามารถลงทะเบียนเพื่อให้คำปฏิเสธที่จะรับโฆษณาใดๆ ไม่ว่าทางอีเมล หรือทางโทรศัพท์ และแจ้งให้ทราบถึงการปฏิเสธเช่นนั้นไปยังธุรกิจการสื่อสารทางสาย และอี-คอมเมิร์ซ เพื่อนำไปเปรียบเทียบ และยืนยันการปฏิเสธของผู้บริโภคที่จะรับข้อความโฆษณาโดยวิธีเหล่านั้น

ส่วนหน่วยงานด้านความปลอดภัยของข้อมูลในเกาหลี หรือ Korea Information Security Agency (KISA) นั้นมีหน้าที่ตรวจสอบทุกคำร้องทุกข์ที่แจ้งว่ามีการละเมิดกฎหมาย ถ้ามีการละเมิดกฎหมายฉบับดังกล่าวที่ชัดเจน KISA ก็สามารถขอให้กระทรวงข้อมูลและการสื่อสารที่จะออกคำสั่งทางบริหาร หรือสั่งปรับ KISA ยังสามารถโอนคดีอาญาไปยังสำนักงานอัยการแห่งชาติได้อีกด้วย KFTC ก็สามารถขอให้ออกคำสั่งทางบริหาร และเรียกค่าปรับเพิ่มได้ โดยผ่านกระบวนการกึ่งศาล และสแปมเมอร์ที่ทำผิดกฎหมายก็จะถูกรายงานไปยังสำนักงานอัยการแห่งชาติ และทั้งกระทรวงข้อมูลและการสื่อสาร และ KFTC สามารถออกคำสั่งบริหาร และค่าปรับสำหรับการละเลยของสแปมเมอร์ที่ผิดกฎหมายด้วย

The Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 ถูกแก้ไขในปี 2002 และ 2003 โดยห้ามนักโฆษณาจากการใช้โปรแกรม หรืออุปกรณ์ทางเทคนิคอื่นๆ ในการสร้าง หรือรวบรวมรายชื่อต่างๆ กฎหมายได้กำหนดโทษปรับสำหรับผู้ที่ฝ่าฝืนเงื่อนไขนี้ด้วย กฎหมายยังได้ห้ามการเก็บเกี่ยวที่อยู่อีเมลจากเวปเพจที่ห้ามการกระทำเช่นนั้นโดยชัดแจ้ง และห้ามการแบ่งปัน การขาย การแลกเปลี่ยน และการจัดให้มีรายชื่อที่เก็บเกี่ยวมาได้

ในการแก้ไขกฎหมายครั้งนี้ยังยอมให้ ISPs มีอำนาจโดยตรงที่จะปฏิเสธการให้บริการถ้ามีข้อสงสัยที่มีเหตุผล และเชื่อมั่นได้ถึงการกีดขวางที่รุนแรง และเกิดขึ้นซ้ำๆ มีสาเหตุมาจากการไหลทะลักเข้ามาจำนวนมากของสแปม ข้อตกลงของ ISPs ต้องอธิบายถึงมาตรการในการเผชิญหน้า และเงื่อนไขในการปฏิเสธการให้บริการเช่นนั้นด้วย

ขณะที่ไม่มีหน่วยงานใดไม่ว่า กระทรวงข้อมูลและการสื่อสาร และ KISA สามารถดำเนินคดีกับสแปมเมอร์จากต่างชาติที่มีเป้าหมายเป็นผู้ใช้อีเมลภายในประเทศ การใช้อย่างผิดๆ ซึ่งคอมพิวเตอร์ส่วนบุคคลของชาวเกาหลี หรือการใช้บริการเมลโดยสแปมเมอร์ต่างชาติก็อาจจะถูกเจาะเข้าโปรแกรมคอมพิวเตอร์อย่างผิดกฎหมายได้

KISA ได้เข้าร่วมในการทำข้อตกลงความเข้าใจ (MOUs) กับองค์กรการสื่อสารของชาวออสเตรเลีย และสำนักงานแห่งชาติเพื่อข้อมูลทางเศรษฐกิจของออสเตรเลียเดิม ซึ่งถูกรวมเข้าไว้ในกระทรวงเทคโนโลยีข้อมูล การสื่อสาร และศิลปะ โดยวางแผนที่จะร่วมมือกันในการต่อต้านสแปมภายใต้เงื่อนไขของกฎหมายของแต่ละประเทศ

**3.7 องค์กรสากลที่จัดตั้งขึ้นเพื่อความร่วมมือในการแก้ไขปัญหาสแปมเมล**

ในปัจจุบัน นอกจากหน่วยงานของรัฐที่มีหน้าที่ในการดูแลเรื่องนี้โดยตรงแล้ว ก็ยังมีองค์กรเอกชนจำนวนมากที่มีวัตถุประสงค์ในการต่อต้านสแปมเมล ทั้งการต่อต้านผู้ที่ทำการสแปม การขึ้นบัญชีผู้ให้บริการ หรือเซิร์ฟเวอร์ที่เป็นต้นตอของการสแปม และการให้ข้อมูลความรู้แก่ผู้ใช้บริการอินเตอร์เนต และจดหมายอิเล็คทรอนิคส์ เกี่ยวกับสแปมเมล ความสำคัญและความรุนแรงของปัญหาและมาตรการในการป้องกันตัวเองในเบื้องต้น อีกทั้งยังเป็นสื่อกลางในการสร้างความร่วมมือระหว่างองค์กรในต่างประเทศ เพื่อศึกษา พูดคุย แลกเปลี่ยนประสบการณ์เกี่ยวกับปัญหาในเรื่องสแปมเมล

องค์กรสากลที่จัดตั้งขึ้น และมีชื่อเสียงเป็นที่รู้จักอย่างมากองค์กรหนึ่งคือ The Coalition Against Unsolicited Commercial Email หรือ CAUCE (http://www.cauce.org/) อันเป็นองค์กรอาสาสมัครทั้งหมด ที่ก่อตั้งโดยผู้ใช้อินเตอร์เนตในสหรัฐฯ โดยเริ่มต้นมาจากกลุ่มสนทนาที่เรียกว่า SPAM-LAW ซึ่งแตกกิ่งก้านสาขาออกมาจากกลุ่มสนทนาที่ชื่อว่า SPAM-L อันเป็นกลุ่มที่สนทนาเกี่ยวกับสแปม และวิธีป้องกัน ผู้เข้าร่วมสนทนาในกลุ่ม SPAM-L จำนวนหนึ่งมีความรู้สึกว่ากฎหมายเป็นสิ่งจำเป็นที่จะหยุดยั้งสแปมจากการคุกคามชีวิตของพวกเขาได้ จึงได้ก่อตั้งกลุ่มสนทนาโดยเฉพาะเกี่ยวกับเรื่องนี้ขึ้นแยกออกมาต่างหากที่เรียกว่า SPAM-LAW อันเป็นทางเลือกในการพูดคุยเกี่ยวกับกฎหมายเพิ่มเติมในการป้องกันสแปม

CAUCE ก่อตั้งขึ้นในปี 1997 สมาชิกหลักของ CAUCE ก็คือสมาชิกของกลุ่ม SPAM-LAW ที่ตระหนักว่าการใช้เทคโนโลยีเพียงอย่างเดียว ไม่สามารถหยุดยั้งสแปมเมลได้ จึงต้องอาศัยกฎหมายเป็นเครื่องมือในการหยุดยั้งสแปมเมล และสนับสนุนการบัญญัติกฎหมายเป็นทางออกในการแก้ไขปัญหาสแปมเมล โดยเสนอให้มีการแก้ไขกฎหมายของรัฐบาลกลาง ที่บัญญัติว่า แฟกซ์ขยะเป็นสิ่งผิดกฎหมาย ให้ครอบคลุมถึงอีเมลด้วย ตั้งแต่นั้นมา CAUCE ก็ได้กลายเป็นกระบอกเสียงสำคัญต่อชุมชนการต่อต้านสแปมเมล

CAUCE นั้นเป็นองค์กรที่ไม่แสวงหากำไร ไม่มีเงินทุน ไม่มีออฟฟิศ และไม่ยอมรับเงินบริจาค เนื่องจากอาจตกอยู่ภายใต้การให้สนับสนุนการออกกฎหมายอีกหลายฉบับ รวมถึงอุปสรรคทางด้านกฎหมาย เทคนิค และทางด้านบัญชีด้วย CAUCE จึงทำงานโดยอาสาสมัครทั้งหมด เท่าที่เวลาและปัจจัยด้านเทคนิคอื่นๆ จะเอื้ออำนวย นอกจากนั้น CAUCE ยังมีเครือข่ายในหลายๆ ทวีปทั่วโลกอันได้แก่

The European Coalition Against Unsolicited Commercial Email

(http://www.euro.cauce.org/en/index.html)

The Canadian Coalition Against Unsolicited Commercial Email

(http://cauce.ca/about.html)

Coalition Against Unsolicited Bulk Email, Australia

(http://www.caube.org.au/)

The Asia Pacific Coalition Against Unsolicited Commercial Email

(http://www.apcauce.org/aboutus/committee.html)

CAUCE India

(http://www.india.cauce.org/)

นอกจากนี้ องค์กรเหล่านี้ ยังได้ร่วมมือกันจัดตั้ง The International Coalition Against Unsolicited Commercial Email หรือ iCAUCE (http://www.international.cauce.org/) เพื่อให้ความช่วยเหลือด้านต่างๆ แก่อาสาสมัครที่ปรารถนาจะดำเนินกิจกรรมเหล่านี้ในประเทศที่ยังไม่มีองค์กรที่ให้การสนับสนุนการออกกฎหมายที่เป็นอิสระด้วย