บทที่ 3

ประเด็นปัญหาและมาตรการแก้ไขปัญหาที่เกี่ยวกับการทำธุรกรรมผ่านทางโทรศัพท์เคลื่อนที่ในต่างประเทศ

1. ประเด็นปัญหาที่เกิดขึ้นในการทำธุรกรรมผ่านทางโทรศัพท์เคลื่อนที่

การทำธุรกรรมผ่านทางโทรศัพท์เคลื่อนที่นั้นก่อให้เกิดผลกระทบต่อผู้ใช้บริการ และทำให้ประเด็นในการคุ้มครองผู้บริโภคต่างๆมีความสำคัญเพิ่มมากขึ้น โดยเฉพาะอย่างยิ่งในเรื่องที่เกี่ยวกับการขายที่ไม่พึงประสงค์อันเกิดขึ้นมาจากการเสนอขาย และการโฆษณาต่างๆที่ส่งมาทาง SMS (SMS Spam) ระดับการเปิดเผยข้อมูลที่ไม่เหมาะสมจากการที่ให้ผู้ให้บริการตกลงยอมรับข้อเสนอต่างๆโดยเพียงแค่ “กดปุ่ม” ตอบกลับ SMS โดยไม่ได้ให้ผู้ใช้บริการเข้าถึงตัวสัญญา หรือให้ข้อมูลเกี่ยวกับสัญญาแต่เพียงบางส่วนแก่ผู้ใช้บริการเท่านั้นซึ่งอาจก่อให้เกิดความเข้าใจผิดแก่ผู้ใช้บริการ และทำให้ผู้ใช้บริการตกลงเข้าทำสัญญาอันไม่ได้มาจากเจตนาที่แท้จริงของผู้ใช้บริการ การคุ้มครองผู้เยาว์ในการทำธุรกรรมทางการเงินต่างๆ และในการเข้าใช้บริการที่ไม่เหมาะสมสำหรับเด็ก รวมทั้งการใช้โดยไม่ได้รับอนุญาตจากการกระทำนอกขอบอำนาจ หรือการใช้โดยบุคคลที่ไม่มีอำนาจเนื่องจากโทรศัพท์เคลื่อนที่หายหรือถูกขโมยไป[1] ขณะที่การพัฒนาทางด้านเทคโนโลยีสามารถแก้ไขประเด็นปัญหาที่กล่าวมาข้างต้นนี้ได้ในบางส่วน แต่ความคุ้มครองทางกฎหมาย การกำกับดูแลตนเองของภาคธุรกิจ และการรณรงค์ให้ข้อมูลแก่ผู้บริโภคก็เป็นส่วนที่สำคัญ[2] ในส่วนนี้จึงมุ่งไปที่มาตรการที่มารองรับปัญหาต่างๆที่ผู้บริโภควิตกกังวลเกี่ยวกับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่[3]

---

[1] เนื้อหาส่วนนี้ใช้ข้อมูลจากคำตอบจากแบบสอบถามเกี่ยวกับปัญหาด้านนโยบายผู้บริโภคที่เกี่ยวข้องกับการค้าเคลื่อนที่ที่มุ่งวิเคราะห์กลไกและความริเริ่มที่ใช้ในการแก้ปัญหาเหล่านั้น ประเทศสมาชิก 19 ประเทศและสหภาพยุโรปได้ตอบรับแบบสอบถามในเดือนกันยายน 2549 โครงการดังกล่าวไม่ได้ครอบคลุมปัญหาด้านการตั้งค่าโทรและค่าธรรมเนียมการส่งข้อความทางโทรศัพท์เคลื่อนที่ จึงไม่ได้กล่าวไว้ในที่นี้

[2] นาง Claire Alexandre จากโวดาโฟน กล่าวในการประชุมคณะกรรมการว่าด้วยนโยบายด้านผู้บริโภค (Committee on Consumer Policy: CCP) ว่า เทคโนโลยีเป็นเพียง

1.1 ปัญหาที่เกิดขึ้นในการทำธุรกรรมผ่านทางโทรศัพท์เคลื่อนที่ในประเทศสมาชิกขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development: OECD)[4]

ในประเทศญี่ปุ่นได้มีการสำรวจผู้บริโภคถึงปัญหาที่วิตกกังวลเกี่ยวกับระบบการชำระเงินทางโทรศัพท์เคลื่อนที่[5] ซึ่งผลการสำรวจออกมาว่าผู้บริโภคมีความกังวลในประเด็นการคุ้มครองข้อมูลส่วนบุคคล 78.2% และการเพิ่มขึ้นของการใช้ไปในทางที่มิชอบ และปัญหาการขโมย 75.9% ซึ่งถือเป็นประเด็นปัญหาที่ใหญ่ที่สุดที่ผู้บริโภคกังวล และจากการที่สหพันธ์ผู้บริโภคสากล (Consumer International: CI) ทำการสำรวจสมาชิกได้แสดงให้เห็นว่า สมาชิกค่อนข้างที่จะวิตกกังวลเกี่ยวกับประเด็นปัญหาดังต่อไปนี้คือ ระดับการเปิดเผยข้อมูลที่ไม่เหมาะสมเกี่ยวกับสินค้าหรือบริการที่เสนอ และเกี่ยวกับค่าใช้จ่ายสุทธิ ซึ่งถูกเรียกเก็บจากการที่บุคคลอื่นใช้โดยปราศจากความรู้เห็นหรือความยินยอมจากผู้ใช้บริการโทรศัพท์เคลื่อนที่ ระดับการเปิดเผยข้อมูลที่ไม่เหมาะสมเกี่ยวกับข้อกำหนดและสภาพเงื่อนไขของค่าบริการ การรักษาความปลอดภัยในการทำ

เครื่องมืออย่างสุดท้ายที่จะสามารถฟื้นฟูความเชื่อมั่นได้ การพัฒนาเทคโนโลยีนั้น สามารถสร้างความโปร่งใส แต่ผู้ที่จะนำมันไปใช้ในทางที่ผิด จะสามารถใช้ได้เร็วกว่า

[3] อ้างถึง Ngai and Gunasekaran (2005) บทความเพียงน้อยชิ้นที่ศึกษาปัญหาด้านกฎหมายและจริยธรรมที่เกี่ยวกับการค้าอุปกรณ์สื่อสารเคลื่อนที่ ดูประกอบ Rawson (2002).

[4] องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา มีประเทศสมาชิก 30 ประเทศ ดังนี้ ประเทศออสเตรเลีย ประเทศออสเตรีย ประเทศเบลเยี่ยม ประเทศแคนาดา ประเทศสาธารณรัฐเช็ก ประเทศเดนมาร์ก ประเทศฟินแลนด์ ประเทศฝรั่งเศส ประเทศเยอรมัน ประเทศกรีซ ประเทศฮังการี ประเทศไอซ์แลนด์ ประเทศไอร์แลนด์ ประเทศอิตาลี ประเทศญี่ปุ่น ประเทศเกาหลี ประเทศลักเซมเบิร์ก ประเทศเม็กซิโก ประเทศเนเธอร์แลนด์ ประเทศนิวซีแลนด์ ประเทศนอรเวย์ ประเทศโปแลนด์ ประเทศโปรตุเกส ประเทศสาธารณรัฐสโลวัก ประเทศสเปน ประเทศสวีเดน ประเทศสวิสเซอร์แลนด์ ประเทศตุรกี ประเทศอังกฤษ ประเทศสหรัฐอเมริกา ดูข้อมูลเพิ่มเติมได้ที่ <www.oecd.org/sti/consumer-policy>.

[5] อ้างถึง MRI & Rakuten (2004).

ธุรกรรมชำระเงินผ่านทางโทรศัพท์เคลื่อนที่ การคุ้มครองข้อมูลส่วนบุคคลเมื่อโทรศัพท์เคลื่อนที่สูญหายหรือถูกขโมย และการปฏิบัติทางการตลาดที่รุนแรงต่อกลุ่มเป้าหมายซึ่งเป็นผู้เยาว์[6]

การสำรวจอีกแหล่งหนึ่งซึ่งจัดทำโดยกลุ่มเจรจาผู้บริโภคสองฟากฝั่งมหาสมุทรแอตแลนติก (Trans Atlantic Consumer Dialogue: TACD) ซึ่งเป็นความร่วมมือกันขององค์กรผู้บริโภคในประเทศสหรัฐอเมริกาและสหภาพยุโรปได้แสดงให้เห็นว่าผู้บริโภคมีความวิตกกังวลเกี่ยวกับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (Mobile Commerce) ที่สำคัญหลายประการ โดยเฉพาะปัญหาที่เกี่ยวกับระดับการเปิดเผยข้อมูลที่ไม่เหมาะสมเกี่ยวกับสินค้าหรือบริการที่ถูกนำเสนอ ข้อกำหนดของการขาย และค่าใช้จ่ายทั้งหมด ปัญหาเรื่องการขายสินค้าที่ไม่พึงประสงค์ (Spam) การคุ้มครองข้อมูลและการรักษาความปลอดภัย และการปรับปรุงแก้ไขกลไกการทำงาน[7]

1.2 **การร้องเรียนของผู้บริโภคในประเทศสมาชิกของ** OECD

ในส่วนการร้องทุกข์ของผู้บริโภคนั้น ประเทศสมาชิกขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development: OECD) บางประเทศยังไม่เคยได้รับการร้องเรียนอย่างเป็นทางการจากผู้บริโภคเกี่ยวกับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (Mobile Commerce) เช่น ประเทศสาธารณรัฐเช็ก ประเทศแคนาดา ประเทศฝรั่งเศส ประเทศแมกซิโก ประเทศโปแลนด์ และประเทศสาธารณรัฐสโลวัก อย่างไรก็ตาม จำนวนของการร้องเรียนเพิ่มสูงขึ้นอย่างเห็นได้ชัดในบางประเทศ อย่างประเทศนอรเวย์ ในปี พ.ศ. 2548 เนื่องจากมีการร้องเรียนจากผู้บริโภคจำนวนมาก กลุ่มพิทักษ์สิทธิผู้บริโภค (Consumer Ombudsman) ต้องจัดการคดีของผู้บริโภคจำนวน 115 คดีที่เกี่ยวกับประเด็นปัญหาบริการเนื้อหาข้อมูลผ่านทางโทรศัพท์เคลื่อนที่ (Mobile Content service) และ 60 คดีที่เกี่ยวกับการโฆษณาที่ไม่ได้รับอนุญาตผ่านทางข้อความสั้น (SMS)

---

[6] รายงานโดยนาง Anna Fielder อดีตผู้อำนวยการสหพันธ์ผู้บริโภคสากล (Consumer International) ในการประชุมเกี่ยวกับค้าการอุปการณ์สื่อสารระหว่างการประชุมคณะกรรมการว่าด้วยนโยบายด้านผู้บริโภค ครั้งที่ 69 ในเดือนมีนาคม พ.ศ. 2548

[7] TACD (2006) เปิดเผยว่า ร้อยละ 38 ของผู้ตอบแบบสอบถามเคยประสบปัญหาเกี่ยวกับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ ในช่วงเวลา 12 เดือน ทั้งยังแสดงให้เห็นว่าเนื้อแท้ของปัญหาผู้บริโภคไม่ถูกสะท้อนอย่างพอเพียงในสถิติของคำร้องต่อรัฐบาล เนื่องจาก ร้อยละ 59 ของผู้ตอบแบบสอบถามไม่เคยแจ้งเรื่องนี้กับใคร มีเพียงร้อยละ 12 เท่านั้นที่ติดต่อกับหน่วยงานรัฐ

ในปัจจุบันการร้องเรียนของผู้บริโภคในประเทศสมาชิกขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development: OECD) สามารถแบ่งออกได้เป็น 3 ประเด็นคือ หนึ่ง ประเด็นเรื่องการขายเนื้อหา (Content) หรือบริการโดยไม่ได้รับอนุญาต สอง ประเด็นเรื่องระดับในการเปิดเผยข้อมูลที่ไม่เหมาะสม และสามประเด็นที่เกี่ยวกับผู้เยาว์ เช่นการตลาดที่ไม่เหมาะสม และการบริโภคมากเกินสมควร

1.2.1 **การขายที่ไม่พึงประสงค์** (Unsolicited sales)

สำหรับกรณีการขายที่ไม่พึงประสงค์นั้น เช่น ผู้บริโภคของประเทศสวิสเซอร์แลนด์ถูกเรียกเก็บเงินจากค่าสัญลักษณ์ (Logos) เสียงเรียกเข้า (Ringtones) และค่าบริการอื่นโดยที่พวกเขาไม่ได้ทำการสั่งซื้อ หรือในประเทศสวีเดนเมื่อผู้บริโภคตอบรับข้อเสนอที่ต้องไม่เสียค่าใช้จ่ายสำหรับเสียงเรียกเข้า (Ringtones) หรือเนื้อหา (Content) อื่นที่คล้ายกัน โดยการส่งข้อความตอบกลับ ซึ่งภายหลังพวกเขาก็ได้รับเนื้อหา (Content) ทุกสัปดาห์ และมีใบเรียกเก็บเงินสำหรับเนื้อหา (Content) ดังกล่าวตามมา และในประเทศฟินแลนด์ ก็มีปัญหาที่คล้ายกัน รวมทั้งการที่กลุ่มพิทักษ์สิทธิผู้บริโภคในประเทศนอรเวย์และประเทศฟินแลนด์ ได้รับการร้องเรียนจำนวนมากเกี่ยวกับระดับการเปิดเผยข้อมูลที่ไม่เหมาะสมเกี่ยวกับราคาค่าบริการเนื้อหาทางโทรศัพท์เคลื่อนที่ (Mobile Content) และความยากลำบากในการตรวจสอบค่าใช้จ่าย ศูนย์กิจการผู้บริโภคแห่งชาติประเทศญี่ปุ่น (National Consumer Affairs Center of Japan: NCAC) ก็ได้รับการร้องเรียนจำนวนมากในเรื่องที่คล้ายกัน ตัวอย่างเช่น เด็กนักเรียนอายุ 17 ปี ได้เข้าไปในเว็บไซต์ที่มีสื่อลามกให้ดูฟรีซึ่งได้ยินมาจากเพื่อน แต่กลับพบข้อความว่า “โปรดจ่ายเงินจำนวน 50,000 เยน (ประมาณ 430 ดอลลาร์สหรัฐ) สำหรับเป็นค่าธรรมเนียมในการใช้เว็บไซต์ของเราภายใน 3 วัน” และเมื่อเขาโทรไปที่ผู้ให้บริการเว็บไซต์ก็ได้ยินแต่เสียงที่บันทึกเอาไว้ที่คอยนำเสนอโปรแกรมลามก หลังจากนั้นเขาก็ได้รับข้อความอีกอันจากผู้ให้บริการที่แจ้งว่า “ถ้าเขาละเลยไม่ใส่ใจใบเรียกเก็บเงิน สิทธิเรียกร้องจะยังมีผลบังคับไปจนกว่าจะได้มีการปฏิบัติการชำระหนี้จนเสร็จสิ้น”

1.2.2 **ระดับการเปิดเผยข้อมูลที่ไม่เหมาะสม**

สำหรับระดับการเปิดเผยข้อมูลที่ไม่เหมาะสมซึ่งมีสาเหตุมาจากข้อจำกัดของหน่วยความจำ และขนาดหน้าจอของโทรศัพท์เคลื่อนที่นั้น ผู้บริโภคในประเทศสมาชิกขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development: OECD) บางประเทศมักได้รับการแสดงข้อตกลงที่เพียงแค่ “กดปุ่ม” และไม่จำเป็นต้องเข้าถึงตัวข้อตกลง หรือไม่ได้รับการแสดงข้อสัญญาฉบับเต็ม ข้อกำหนดและเงื่อนไข

ต่างๆที่ครอบคลุมเนื้อหาในข้อตกลง หรือรายละเอียดต่างๆที่เกี่ยวกับกระบวนการทำงาน วิธีการใช้ก่อนที่จะตกลงเข้าทำข้อตกลง กลุ่มพิทักษ์สิทธิผู้บริโภคแห่งนอรเวย์ (Norwegian Consumer Ombudsman) ก็ได้รับการร้องเรียนจำนวนมากเกี่ยวกับความไม่เพียงพอของข้อมูลในส่วนที่เกี่ยวกับราคาของค่าบริการเนื้อหาทางโทรศัพท์เคลื่อนที่ (Mobile Content) และความยากในการตรวจสอบค่าใช้จ่ายต่างๆ

1.2.3 ประเด็นความรับผิดในการชำระเงิน

ในการสำรวจของกลุ่มเจรจาผู้บริโภคสองฟากฝั่งมหาสมุทรแอตแลนติก[8] (Trans Atlantic Consumer Dialogue: TACD)[9] ยังชี้ให้เห็นว่าปัญหาส่วนใหญ่ที่ได้รับการร้องเรียนมาซึ่งเกี่ยวกับการชำระเงินผ่านทางโทรศัพท์เคลื่อนที่นั้นเป็นเรื่องของการที่ราคาสินค้าหรือบริการไม่ตรงกับความเป็นจริง หรือมีความผิดพลาด ร้อยละ 35 ในส่วนที่เกี่ยวกับประเด็นความรับผิดในการชำระเงินนั้น ผู้บริโภคหลายรายในประเทศ ฟินแลนด์ถูกบังคับให้ต้องรับผิดโดยบริษัทที่ปล่อยกู้เงินด่วน แม้ว่าพวกเขาจะไม่ได้เป็นผู้ทำการกู้เงินก็ตาม ปัญหาดังกล่าวเกิดขึ้นเนื่องจากบุคคลใดๆ สามารถที่จะทำการกู้เงินดังกล่าวออกมาโดยใช้การส่งข้อความในชื่อของบุคคลอื่นได้ โดยเพียงแค่ใช้เบอร์โทรศัพท์เคลื่อนที่และเลขรหัสประจำตัว (ID) ของบุคคลนั้น แต่บริษัทดังกล่าวกลับไม่ได้มีการตรวจสอบหลักฐานต่างๆที่แสดงว่าเป็นบุคคลผู้นั้นของผู้ส่ง[10]

1.2.4 ผู้เยาว์

ในส่วนที่เกี่ยวกับผู้เยาว์นั้น มีตัวอย่างเช่น กลุ่มพิทักษ์สิทธิผู้บริโภคแห่งฟินแลนด์ (Finnish Consumer Ombudsman) ได้รับรายงานจำนวนมากจากผู้ปกครองซึ่งได้รับใบแจ้งหนี้ค่า

---

[8] กลุ่ม Transatlantic Consumer Dialogue หรือ TACD คือกลุ่มเจรจาผู้บริโภคสองฟากฝั่งมหาสมุทรแอตแลนติก ซึ่งเป็นการรวมตัวของกลุ่มผู้บริโภค

[9] อ้างถึง TACD (2006).

[10] บริการให้กู้แบบด่วนเป็นปัญหาด้านการตลาดตั้งแต่เริ่มต้นเนื่องด้วยข้อเท็จจริงที่ว่าไม่มีการกล่าวไว้ในสัญญาว่าผู้บริโภคจะสามารถยกเลิกการให้กู้ดังกล่าวได้ ฉะนั้น จึงจะทำให้เกิดปัญหาตามมาคือ บริษัทผู้ให้บริการไม่ได้แจ้งข้อมูลที่เพียงพอแก่ผู้ใช้หรือในสัญญา ถึงแม้ว่าจะสามารถใช้การส่งข้อความก็ได้, ดูข้อมูลเพิ่มเติมได้ที่ <Uutiskirje.kuluttajavirasto.fi/consumer_law/consumer_law_4_2006/en_GB/instant_loans/>.

โทรศัพท์เคลื่อนที่ที่ต้องจ่ายหลายร้อยยูโร เพราะลูกของพวกเขาเข้าใช้บริการเกมโทรทัศน์ที่สามารถโต้ตอบกันได้ (Interactive TV Games) และโปรแกรมสนทนาต่างๆ (Chat Programs) โดยการส่งข้อความ ซึ่งกลุ่มพิทักษ์สิทธิผู้บริโภคแห่งเดนมาร์ก (Danish Consumer Ombudsman) ก็ได้รับการร้องเรียนในเรื่องต่างๆที่คล้ายคลึงกัน

1.2.5 **อื่น ๆ**

การร้องเรียนอื่นๆนั้นเกี่ยวกับการไม่ได้รับเนื้อหาทางโทรศัพท์เคลื่อนที่ (Mobile Content) ที่สั่งไป ความยากในการเข้าใจและ/หรือความไม่เป็นธรรมของกระบวนการทำงาน ความไม่ปลอดภัยในการทำธุรกรรมต่างๆผ่านทางโทรศัพท์เคลื่อนที่ และข้อบกพร่องทางเทคนิคอื่นๆของระบบเครือข่ายโทรคมนาคมผ่านโทรศัพท์เคลื่อนที่ และปัญหาที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ส่วนปัญหาการขายสินค้าที่ไม่พึงประสงค์ (Spam) ผ่านโทรศัพท์เคลื่อนที่ก็เป็นปัญหาใหญ่เช่นเดียวกัน[11]

กรณีการร้องเรียนที่เกี่ยวกับการบริการข้ามประเทศกลายเป็นสิ่งที่พบมากขึ้นในประเทศสมาชิกขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development: OECD) ยกตัวอย่างเช่น ผู้บริโภคชาวฟินแลนด์ได้รับข้อเสนอสำหรับเสียงเรียกเข้า (Ringtones) ฟรีจากผู้ทำธุรกิจในอีกประเทศหนึ่งที่เป็นการหลอกลวง อีกกรณีที่สำคัญนั้นเกี่ยวพันกับการขโมยอุปกรณ์เครื่องมือสื่อสารในประเทศญี่ปุ่น[12] ตัวอย่างเช่น ผู้หญิงชาวญี่ปุ่นได้นำโทรศัพท์เคลื่อนที่ไปต่างประเทศด้วยเพื่อใช้เป็นกล้องถ่ายภาพดิจิตอล และมันได้ถูกขโมยไป เธอได้ไปแจ้งต่อตำรวจท้องถิ่น แต่ไม่ได้ทำการแจ้งไปยังบริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่โดยทันที เพราะในคู่มือของบริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่ระบุว่าโทรศัพท์เคลื่อนที่เครื่องนั้นสามารถใช้ได้ภายในประเทศเท่านั้น ทำให้เธอเข้าใจว่ามันไม่สามารถที่

---

[11] อ้างถึง Rettie et al (2005) การโฆษณาทางข้อความบนโทรศัพท์เคลื่อนที่ได้ผลดีกว่าการส่งตรงทางไปรษณีย์หรือการตลาดผ่านอีเมล์บนอินเตอร์เน็ต จะเห็นได้จากอัตราการตอบรับถัวเฉลี่ยร้อยละ 31 จาก 26 บริษัท ดังนั้น ด้วยการใช้ข้อมูลพื้นที่ การโฆษณาเชิงรุกสามารถโฆษณาแก่ผู้รับบริการในพื้นที่ใกล้เคียงผ่านโทรศัพท์เคลื่อนที่ได้ ตามตัวอย่างใน www.yellowmap.com/english/lba.asp, www.blueblitz.com, www.toroblue.com และ www.ad2hand.com รูปแบบที่ซับซ้อนของการโฆษณาผ่านโทรศัพท์เคลื่อนที่โดยการใช้สื่อผสม เช่น วีดิทัศน์ และโทรทัศน์ดิจิตอลอยู่ระหว่างการนำมาทดลองตลาด.

[12] อ้างถึง NCAC (2006).

จะใช้งานในต่างประเทศได้ แต่ต่อมาภายหลังเธอถูกเรียกเก็บเงินประมาณ 3 ล้านเยน (ประมาณ 25,600 ดอลลาร์สหรัฐ) เพราะตัวบัตรเก็บข้อมูล (IC Card)[13] ของเธอถูกย้ายออกจากเครื่อง ไปใส่ในโทรศัพท์เคลื่อนที่อีกเครื่องหนึ่ง ซึ่งสามารถใช้งานในต่างประเทศได้ เนื่องจากโทรศัพท์เคลื่อนที่นั้นมีระบบการชำระเงินแบบผสมผสาน สามารถให้บริการเบ็ดเสร็จ ณ จุดเดียว (One-stop Platforms) และสามารถทำงานข้ามระบบ (Cross-over Platforms) ได้อีกด้วยโดยทำหน้าที่เป็นเสมือนทั้งเงินอิเล็กทรอนิกส์ เงินชำระล่วงหน้า (Prepaid Money) เครดิตการ์ด บิลค่าโทรศัพท์ (Telephone Bills) เป็นต้น ขึ้นอยู่กับประเภทการใช้งานหรือธุรกิจ ทำให้มาตรการในการคุ้มครองอาจแตกต่างกันไป และทำให้ความเสี่ยงที่จะถูกขโมยโทรศัพท์เคลื่อนที่และถูกนำไปใช้โดยมิชอบเพิ่มสูงขึ้น[14]

การขโมยโทรศัพท์เคลื่อนที่นั้นโดยแท้จริงแล้วเป็นประเด็นที่แพร่หลายทั่วโลก เนื่องจากแรงจูงใจทางเศรษฐกิจที่จะขโมยข้อมูลส่วนบุคคลและข้อมูลทางการเงิน จากที่กล่าวมา

---

[13] บัตร Integrated Circuit Card (IC Card) เป็นวิทยาการใหม่ที่มีแนวโน้มใช้ทดแทนตั๋วแถบแม่เหล็กได้ด้วยศักยภาพในการบรรจุข้อมูลมากกว่าเดิม 100 เท่า อีกทั้งสามารถส่งผ่านข้อมูลด้วยความไวเพียง 0.02 วินาที ซึ่งจากผลการทดสอบในภาคสนามทั้ง 3 ครั้งได้ข้อสรุปถึงรูปแบบ IC Card ที่ทำงานโดยสัมผัสกับเครื่องอ่านตั๋วโดยตรงแล้วส่งผลและรับสัญญาณครึ่งทรงกลมรัศมี 10 เซนติเมตร ในลักษณะ "Touch and Go" ซึ่งภายในเศษเสี้ยววินาทีของการสัมผัสนั้น ข้อมูลจะถูกส่งผ่านระหว่าง IC Card กับเครื่องด้วยความแม่นยำสูงมากเพื่อคิดค่าโดยสารและเขียนข้อมูลใหม่ทับลงไปแทนที่เรียกว่า non-contact read/write process

กลไกของ IC Card นั้นแตกต่างจากตั๋วแถบแม่เหล็กซึ่งทำงานแบบอ่านอย่างเดียว (read only) โดยข้อมูลบนตั๋วจะถูกส่งไปที่คอมพิวเตอร์กลาง เพื่อตรวจสอบความถูกต้องก่อนประมวลผลกลับมาในลักษณะเดียวกับการซื้อของด้วยบัตรเครดิตโดยเฉพาะในชั่วโมงเร่งด่วน มิใช่ว่าการผ่านเข้าออกสถานีจะรวดเร็วขึ้นเพียงอย่างเดียว ที่สำคัญกว่านั้นคือผู้โดยสารไม่จำเป็นต้องเสียเวลาหยิบตั๋วออกจากกระเป๋าซึ่งโอกาสที่จะทำตั๋วหายนั้นแทบไม่มีเลย นอกจากจะปรับปรุงคุณภาพการบริหารดีขึ้นแล้ว ยังสามารถลดต้นทุนการผลิตตั๋วจำนวนมหาศาลในแต่ละวันลงได้อีกด้วย, ที่มา : ผู้จัดการ ฉบับเดือนเมษายน 2550.

[14] รายงานก่อนหน้าเกี่ยวกับบัตรจ่ายเงินยังกล่าวว่า ประเด็นสำหรับการทดสอบต่อไปในอนาคตคือระบบกฎหมายและการควบคุมจะสามารถประยุกต์กับระบบการจ่ายเงินอื่นๆ อย่างไร หากระบบดังกล่าวถูกนำมาใช้อย่างแพร่หลายโดยผู้บริโภค โดยเฉพาะการจ่ายเงินออนไลน์ (OECD 2001 p. 15).

ข้างต้นระดับที่เพิ่มสูงขึ้นของการนำโทรศัพท์เคลื่อนที่ไปใช้โดยมิชอบ และการขโมยนั้นเป็นหนึ่งในปัญหาที่ใหญ่ที่สุดสำหรับผู้ใช้โทรศัพท์เคลื่อนที่ เนื่องจากมากกว่าครึ่งหนึ่งของอาชญากรรมบนท้องถนน จำนวน 4,000 รายในลอนดอนทุกเดือนมาจากการขโมยโทรศัพท์เคลื่อนที่ และมี 1,200 กรณีที่อุปกรณ์เชื่อมต่อหูฟัง (Handset) ของเหยื่อเป็นเป้าหมายในการขโมย[15] ในประเทศอังกฤษนั้นมีรายงานว่าโทรศัพท์เคลื่อนที่จำนวน 10,000 เครื่องถูกขโมยไปทุกเดือน และในรายงานการค้นคว้าของ Juniper (2006b) ได้คาดการณ์ว่าจำนวนของโทรศัพท์เคลื่อนที่ที่ถูกขโมยจะเพิ่มขึ้นมากกว่าสองเท่าในเอเชียแปซิฟิก และเป็นสองเท่าในอเมริกาเหนือในช่วง 5 ปีข้างหน้า ดังนั้นการป้องกันข้ามชาติสำหรับการใช้โดยไม่ได้รับอนุญาตจะกลายเป็นประเด็นปัญหาที่มีความสำคัญ

1.3 องค์กรระหว่างประเทศที่เกี่ยวข้องกับธุรกิจโทรศัพท์เคลื่อนที่

1.3.1 Organization for Economic Co-operation and Development (OECD)

องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) เป็นองค์กรหนึ่งที่มีความสำคัญระดับโลก มีวัตถุประสงค์เป็นเวทีการเจรจาเพื่อการพัฒนากลั่นกรองนโยบายทางเศรษฐกิจและสังคมของประเทศสมาชิก รวมทั้งประสานงานและช่วยเหลือประเทศสมาชิกและไม่ใช่สมาชิกในการจัดการแก้ไขปัญหาต่างๆในยุคโลกาภิวัตน์ บนพื้นฐานของการศึกษาวิจัยอย่างรอบคอบและเป็นกลาง เพื่อนำไปสู่ข้อสรุปร่วมระดับนโยบายในลักษณะ Guidelines for best practices และการปรับเปลี่ยนนโยบายภายในประเทศสมาชิกให้สอดคล้องกับ guidelines เหล่านั้น

ภารกิจหลัก ได้แก่ การจัดทำนโยบายที่เน้นการช่วยเหลือรัฐสมาชิกให้บรรลุถึงการเจริญเติบโต การจ้างงาน และยกระดับความเป็นอยู่ที่ยั่งยืน ภายใต้เงื่อนไขของการคลังที่มีเสถียรภาพ ผ่านการค้าบนพื้นฐานของความเท่าเทียมกัน นอกจากนี้ องค์กรความร่วมมือและพัฒนาทางเศรษฐกิจ (OECD) ได้พัฒนากรอบนโยบายเพื่อส่งเสริมให้เกิดวัฒนธรรมในเรื่องความปลอดภัยและความเป็นส่วนตัว อีกทั้ง ยังพยายามก่อให้เกิดความไว้วางใจในเรื่องเทคโนโลยีสารสนเทศและการสื่อสาร (ICTs) มาเป็นระยะเวลาหลายปี และการสร้างกรอบดังกล่าวยังเป็นผลให้เกิดการวิเคราะห์และพิจารณาในประเด็นที่เกี่ยวข้องอื่นๆตามมาอีกด้วย

---

[15] อ้างถึง Juniper Research (2006b).

1.3.2 Consumers International (CI)

สหพันธ์ผู้บริโภคสากล (CI) เป็นกลุ่มองค์กรอิสระที่ทำงานด้านการคุ้มครองผู้บริโภค ทำหน้าที่รับเรื่องราวร้องทุกข์จากผู้บริโภคทั่วโลกโดยไม่แสวงหาผลกำไร มีประเทศสมาชิกในเครือข่ายองค์กร 115 ประเทศ องค์กรนี้ก่อตั้งขึ้นตั้งแต่ปี ค.ศ. 1960 (พ.ศ. 2503) ทำหน้าที่ช่วยคุ้มครองผู้บริโภคให้ได้รับความปลอดภัยจากการบริโภคสินค้าและบริการ โดยมีวิสัยทัศน์คือ เป็นองค์กรที่ช่วยพิทักษ์สิทธิของผู้บริโภค[16] โดยองค์กรมองว่าผู้บริโภคทุกคนควรได้รับสินค้าและการบริการที่มีความเหมาะสมและปลอดภัย และองค์กรก็จะกระทำการต่างๆเพื่อให้ผู้บริโภคได้รับสินค้าและบริการที่ดี

1.3.3 The International Telecommunication Union (ITU)

สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ก่อตั้งขึ้นมาตั้งแต่ปลายศตวรรษที่ 19 ค.ศ.1865 (พ.ศ. 2408) ที่กรุงปารีส ประเทศฝรั่งเศส ในชื่อเดิมว่า "สหภาพโทรเลขระหว่างประเทศ" (International Telegraph Union) ต่อมาในปี ค.ศ. 1934 (พ.ศ. 2477) จึงเปลี่ยนชื่อใหม่เป็น "สหภาพโทรคมนาคมระหว่างประเทศ" (ITU) และได้กลายเป็น องค์การชำนาญพิเศษของสหประชาชาติ (United Nations) หรือ UN ในปี ค.ศ.1947 (พ.ศ. 2490) เป็นต้นมา

---

[16] สิทธิของผู้บริโภคตามคำจำกัดความของ Consumers International (CI) ได้แก่

1. สิทธิที่มีความพึงพอใจในความต้องการพื้นฐาน เช่น ได้รับสินค้าและบริการที่มีความจำเป็น มีอาหาร เครื่องนุ่งห่มที่พอเพียงต่อการดำรงชีวิต ได้รับบริการทางสาธารณสุข ได้รับการศึกษา ได้รับสิ่งอำนวยความสะดวกจากภาครัฐ

2. สิทธิที่จะได้รับความปลอดภัยจากการบริโภคสินค้าและบริการ

3. สิทธิในการได้รับข้อมูลข่าวสารต่างๆ ผู้บริโภคมีสิทธิที่จะรับทราบข้อมูลที่ถูกต้อง เพื่อช่วยในการตัดสินใจเลือกบริโภคสินค้าและบริการ

4. สิทธิในการเลือกบริโภคสินค้าและบริการ

5. สิทธิในการรับรู้รับฟังข้อมูลของสินค้าและบริการเพื่อช่วยในการตัดสินใจเลือกใช้สินค้าและบริการดังกล่าว

6. สิทธิในการได้รับความเป็นธรรมจากการใช้สินค้าและบริการ

7. สิทธิที่ผู้บริโภคจะได้รับการพิทักษ์สิทธิของตนจากการบริโภคสินค้าและบริการ

8. สิทธิที่ผู้บริโภคจะได้อาศัยอยู่ในสิ่งแวดล้อมที่ดี

สหภาพโทรคมนาคมระหว่างประเทศ (ITU) เป็นองค์กรระหว่างประเทศที่เกิดขึ้น มาจากความร่วมมือของรัฐบาลประเทศสมาชิกในอันที่จะทำให้เกิดความร่วมมือกัน เพื่อรับผิดชอบด้านการกำกับดูแล (Regulation) การจัดทำมาตรฐาน (standardization) และการพัฒนากิจการโทรคมนาคมของโลก รวมทั้ง การบริหารและจัดการระหว่างประเทศในเรื่องที่เกี่ยวกับสเปกตรัมความถี่วิทยุ (radiofrequency spectrum) ตลอดจนกฎเกณฑ์ต่างๆ ที่จะนำเอาไปใช้สำหรับควบคุมการเข้าถึง (Access to) และการใช้ประโยชน์ (Use) จากวงโคจรดาวเทียม (satellite orbits) ทั้งหลายของประเทศต่างๆ

วัตถุประสงค์หลักโดยทั่วไป ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ประกอบด้วย

1. เพื่อให้มีการพัฒนาและดำรงไว้ซึ่งความร่วมมือระหว่างประเทศของมวลสมาชิกในอันที่จะให้มีการวิวัฒนาการ และการใช้ประโยชน์เกี่ยวกับระบบและชนิดต่างๆ ของกิจการสื่อสาร โทรคมนาคม อย่างเหมาะสม

2. เพื่อส่งเสริม และให้ความช่วยเหลือด้านเทคนิค ต่อประเทศกำลังพัฒนา เรื่องที่เกี่ยวกับกิจการสื่อสาร โทรคมนาคม รวมถึงการส่งเสริมการดำเนินการด้านต่างๆ และด้านเงินทุนที่จำเป็นสำหรับใช้ดำเนินการให้บรรลุผลสำเร็จ

3. เพื่อส่งเสริมให้มีการพัฒนาในส่วนของคุณสมบัติต่างๆ ของเทคโนโลยีใหม่ๆ ทางด้านกิจการสื่อสารโทรคมนาคม ทั้งนี้เพื่อให้มีการพัฒนาทางด้านการควบคุม และ/หรือการใช้งานอย่างเกิดประสิทธิภาพมากที่สุด รวมทั้งเป็นการส่งเสริมให้มีการประดิษฐ์คิดค้นเทคโนโลยีใหม่ๆ อีกด้วย

4. เพื่อส่งเสริมให้มีการกระจายการใช้ประโยชน์ต่างๆ ของเทคโนโลยีสื่อสารโทรคมนาคมที่ทันสมัยไป (เช่น บริการโทรคมนาคมพื้นฐานที่หลากหลาย และบริการเสริมอื่นๆ ตามความต้องการ) ไปสู่มวลมนุษยชาติ

5. เพื่อที่จะส่งเสริมให้มีการใช้ประโยชน์ จากการให้บริการสื่อสารโทรคมนาคม ในการเสริมสร้างความสัมพันธ์อย่างสันติวิธี

6. เพื่อเป็นศูนย์กลางในการประสานงานการดำเนินกิจกรรมต่างๆ ของมวลสมาชิก เพื่อจักได้บรรลุตามเป้าหมายหรือวัตถุประสงค์ที่ได้วางไว้

1.3.4 Mobey Forum

Mobey Forum ก่อตั้งในเดือนพฤษภาคม ปี 2000 โดยสถาบันทางการเงินชั้นนำของโลกและผู้ผลิตโทรศัพท์เคลื่อนที่ (ธนาคาร ABN-AMRO, HSBC, Nokia, Nordea และ USB) โดยมีเป้าหมายเพื่อกระตุ้นการใช้บริการทางการเงินผ่านเทคโนโลยีโทรศัพท์เคลื่อนที่

ตั้งแต่ Mobey Forum ก่อตั้งขึ้นมา ก็ได้ทำงานอย่างต่อเนื่องเพื่อบรรลุเป้าหมาย หนึ่งในเรื่องที่ประสบความสำเร็จคือการประกาศ Preferred Payment Architecture ในเดือนมิถุนายน พ.ศ. 2544 ที่ประกอบไปด้วยข้อมูลที่อธิบายแง่มุมทั้งเชิงเทคนิคและเชิงธุรกิจเกี่ยวกับการให้บริการที่เป็นมิตรกับผู้ใช้บริการ (user-friendly) และการรักษาความปลอดภัยในการให้บริการชำระเงินและบริการธนาคารผ่านทางโทรศัพท์เคลื่อนที่ (secure mobile banking and payment service) และในเดือนกันยายน พ.ศ. 2545 ทาง Mobey Forum ได้ตีพิมพ์ Preferred Payment Architecture สำหรับการจ่ายเงินในท้องถิ่น (Local Payments) และสาธิตการทำธุรกรรมทางโทรศัพท์เคลื่อนที่ในท้องถิ่น (local mobile transactions)

บนหลักการของ Preferred Payment Architecture ทาง Mobey Forum ได้ตีพิมพ์ White Paper on Mobile Financial Service ในเดือนมิถุนายน 2003 White paper จะมองไปที่บริการทางการเงินผ่านโทรศัพท์เคลื่อนที่ในสภาพแวดล้อมทางเทคโนโลยีในปัจจุบันและที่ที่เปลี่ยนไป ในปี พ.ศ. 2548 Mobey Forum ได้เสนอกุญแจสำคัญจากการวิเคราะห์ทางเทคนิคคือองค์ประกอบทางด้านความปลอดภัยของอุปกรณ์โทรศัพท์เคลื่อนที่

1.3.5 Mobile Payment Forum

องค์กรนี้เป็นองค์กรระดับโลกที่ประกอบด้วยหลายสถาบัน ก่อตั้งในเดือนพฤศจิกายน พ.ศ.2544 เพื่อที่จะสร้างกรอบสำหรับความพร้อมในเรื่องความง่าย ความปลอดภัย และ ความสามารถในการทำงานร่วมกันได้ในการชำระเงินผ่านโทรศัพท์เคลื่อนที่ (m-payments) องค์กรนี้ก่อให้เกิดสภาวะการเปิดกว้าง ความยืดหยุ่น และความไว้วางใจ ซึ่งสมาชิกมีโอกาสที่จะชี้แจงเกี่ยวกับโอกาสและตั้งประเด็นความท้าทายที่ต้องเผชิญในอุตสาหกรรม

สมาชิกขององค์กรนี้ประกอบไปด้วยองค์กรที่ทำธุรกิจเกี่ยวข้องกับการจ่ายเงินผ่านโทรศัพท์เคลื่อนที่ เช่น สถาบันทางการเงิน (Financial institutions) บริษัทบัตรชำระเงิน (payment card companies) ผู้ประกอบกิจการโทรคมนาคม (telecommunications operators) ผู้ผลิตอุปกรณ์ไร้สาย (wireless-device manufacturers) ร้านค้า (merchants) และผู้ให้บริการด้านเนื้อหา (content providers) ผู้พัฒนาและผู้ขายซอฟแวร์และฮาร์ดแวร์ (software and hardware developers and vendors)

ภารกิจของ Mobile Payment Forum คือ การนำความคิดเห็นของผู้เชี่ยวชาญจากผู้มีส่วนร่วมที่สำคัญในอุตสาหกรรมการติดต่อสื่อสารทางโทรศัพท์เคลื่อนที่และอุตสาหกรรมการเงินมาสร้างพื้นฐานสำหรับมาตรฐานทางเทคโนโลยีและการทำงานของการชำระเงินทางโทรศัพท์เคลื่อนที่ ในการจัดการปัญหาด้วยวิธีดังกล่าวผู้บริโภคและร้านค้าต้องการความง่าย ความปลอดภัย และความสามารถทำงานร่วมกันได้ของทางเลือกในบริการชำระเงินผ่านโทรศัพท์เคลื่อนที่ (m-payment choices) ขณะนี้ Mobile Payment Forum กำลังวางโครงสร้างการชำระเงินทางโทรศัพท์เคลื่อนที่ โดยมีคู่มือสำหรับการพิสูจน์ตัวตนในบริการชำระเงินผ่านโทรศัพท์เคลื่อนที่ (mobile payment authentication) และการรักษาความปลอดภัย และการวางโครงสร้างพื้นฐานที่สามารถทำงานร่วมกันได้สำหรับกระบวนการชำระเงิน ในปัจจุบันคณะกรรมการบริหารได้แก่ VISA international, MasterCard International, Nokia, Vodafone, Telecom Italia Mobile, Sprint, First Data International

1.3.6 Mobile Electronic transactions (MeT)

MeT ก่อตั้งในปี พ.ศ. 2543 โดยบริษัทผู้ผลิตโทรศัพท์เคลื่อนที่ยักษ์ใหญ่จำนวนหนึ่ง ตั้งแต่มีการก่อตั้ง MeT ได้เปลี่ยนแปลงเป้าหมายเริ่มแรกไปเล็กน้อย โดยในช่วงปีแรกๆจะมุ่งเน้นไปที่การพัฒนาข้อจำกัดทางเทคนิคสำหรับการทำธุรกรรมระยะไกล (remote transactions) และสร้างความร่วมมือที่ใกล้ชิดขึ้นระหว่างผู้ขายในอุตสาหกรรมแฮนด์เซ็ต (handset) ภายหลังได้เปลี่ยนมามุ่งเน้นที่การพัฒนาไปสู่ proximity transactions เช่น การชำระเงินในระดับท้องถิ่น (local payments) การออกตั๋วในระบบขนส่งมวลชน (mass transit ticketing) และการโฆษณา ซึ่งทำให้เป็นไปได้โดย Near Field Communication ตั้งแต่ต้นปี พ.ศ. 2548 MeT และสมาชิกได้เข้าร่วมใน NFC Forum เพื่อที่จะรวมข้อกำหนดสำคัญคือ ความสะดวกในการใช้งาน (usability) การรักษาความปลอดภัย (security) และขีดความสามารถในการทำงานระหว่างระบบ (interoperability) ไว้ในกลุ่มสำหรับข้อจำกัดทางด้านเทคนิค สมาชิกกลุ่มนี้ประกอบไปด้วย Ericsson, Nokia, NEC และ Panasonic

1.3.7 Mobile Entertainment Forum (MEF)

MEF เป็นสมาคมการค้าระดับโลก (global trade association) มีขึ้นเพื่อนำเสนอสิ่งที่สมาชิกในอุตสาหกรรมความบันเทิงบนโทรศัพท์เคลื่อนที่ (mobile entertainment value chain) จากทั่วโลกให้ความสนใจ โดยมีจุดประสงค์เพื่อกระตุ้นให้เกิดความตระหนักรู้ สร้างโอกาสในการพัฒนาธุรกิจ รวมถึงพัฒนาแนวทางการโฆษณาและวิธีที่เหมาะสมในการสร้างอุตสาหกรรมที่

แข็งแกร่งและสามารถทำกำไรได้ องค์กรนี้ก่อตั้งเมื่อเดือนกุมภาพันธ์ พ.ศ. 2544 โดย 6 องค์กร คือ Booz, Allen & Hamilton, Cash-U, Comverse, mblox, OpenMobile และ Picofun ที่มีหน้าที่ในการลดอุปสรรคในการเข้าถึงตลาดนวัตกรรมความบันเทิงทางโทรศัพท์เคลื่อนที่ (innovative mobile entertainment market) ซึ่งส่งเสริมการเข้าถึงโดยธุรกิจใหม่ และเพิ่มการแข่งขัน และพัฒนาไปสู่ผลประโยชน์ของผู้ประกอบธุรกิจและผู้บริโภค วัตถุประสงค์ขององค์กรคือ 1.สนับสนุนและผลักดัน 2.สร้างความตระหนัก (awareness) และ 3.สร้างคู่มือ (guideline) ในปัจจุบันบอร์ดบริหารประกอบไปด้วย Amobee, mblox, Eyeka, Sony BMG, Denton Wilde Sapte, Acatel, Vodafone, EMI Music, France Telecom, Beep science และ Sun Microsystems

1.3.8 Open Mobile Alliance (OMA)

OMA ซึ่งตั้งขึ้นในเดือนมิถุนายน พ.ศ. 2545 โดยบริษัทเกือบ 200 บริษัท รวมถึงผู้นำโลกในการประกอบกิจการโทรศัพท์เคลื่อนที่ (world's leading mobile operators) ผู้จัดหาอุปกรณ์และเครือข่าย (device and network suppliers) บริษัทเทคโนโลยีสารสนเทศ (information technology companies) และผู้ให้บริการด้านเนื้อหาและบริการ (content and service providers) ข้อเท็จจริงซึ่งเป็น value chain ทั้งหมดถูกแสดงใน OMA ได้แสดงให้เห็นว่ามีการเปลี่ยนแปลงของบริการโทรศัพท์เคลื่อนที่ในทางข้อจำกัดไปจากวิธีการดั้งเดิมของกิจกรรมขององค์กร คือ "technology silos" ด้วยมาตรฐานที่แตกต่างและส่วนประกอบของข้อกำหนดทางเทคนิค (specifications bodies) แสดงให้เห็นถึงเทคโนโลยีโทรศัพท์เคลื่อนที่ซึ่งทำงานโดยตนเองที่หลากหลาย ทั้งนี้ OMA มีเป้าหมายที่จะรวมทุก specification activities ใน service-enabler space เป็นหนึ่งในองค์กรเดียว

OMA เป็นองค์กรที่สำคัญในการพัฒนาข้อกำหนดทางเทคนิคที่ช่วยส่งเสริมบริการทางโทรศัพท์เคลื่อนที่ (mobile service enabler specifications) ซึ่งสนับสนุนการสร้าง interoperable end-to-end mobile services โดยผลักดันสถาปัตยกรรมที่ส่งเสริมบริการ (service enabler architectures) และเปิด enabler interfaces ของเครือข่ายและระบบไร้สายที่จำเป็น (underlying wireless networks and platforms) ซึ่งเป็นอิสระ OMA สร้างบริการข้อมูลทางโทรศัพท์ที่ทำงานร่วมกันได้ (interoperable mobile data service) ที่ส่งเสริมการทำงานข้ามอุปกรณ์ (devices) ผู้ให้บริการ (service providers) ผู้ประกอบกิจการ (operators) เครือข่าย (networks) และภูมิศาสตร์ (geographies) และออก Interoperable DRM ฉบับ 2.0 ในเดือนเมษายน พ.ศ. 2549 OMA จะพัฒนาข้อกำหนดทางเทคนิคในการทดสอบ (test specifications)

สนับสนุนการพัฒนาเครื่องมือของบุคคลที่สาม (third-party tool development) และจัดการ test activities ซึ่งอนุญาตให้ผู้ขายตรวจสอบการทดลองปฏิบัติของพวกเขา

ในการพัฒนาของ OMA การรวมเป็นหนึ่งที่สำคัญได้รับความสำเร็จด้วยการรวมเข้าด้วยกันใน OMA ของ WAP Forum, Location Interoperability Forum (LIF), SyncML Initiative, MMS-IOP (Multimedia Messaging Interoperability Process), Wireless Village, Mobile Gaming Interoperability Forum (MGIF) และ Mobile Wireless Internet Forum (MWIF) ในการช่วยให้ end-to-end Interoperability ข้ามความแตกต่างของอุปกรณ์ (devices) ภูมิศาสตร์ (geographies) ผู้ให้บริการ (service providers) ผู้ประกอบกิจการ (operators) และเครือข่าย (networks) และยังช่วยสนับสนุนตลาดของ OMA และข้อกำหนดของผู้ใช้ที่มุ่งแนะนำข้อกำหนดทางเทคนิคในการทำงาน (specification work)

1.3.9 GSM Association (GSMA)

สมาคมจีเอสเอ็ม (GSM Association) ก่อตั้งขึ้นเมื่อปี 1987 โดยผู้ปฏิบัติการ 15 รายที่เป็นสมาชิกในกลุ่ม ต่างให้คำมั่นว่าจะส่งเสริมเทคโนโลยีเพื่อรองรับระบบดิจิตอลระหว่างพรมแดนเพื่อการสื่อสารโดยโทรศัพท์เคลื่อนที่ สมาคมดังกล่าวเป็นสมาคมการค้าของโลกที่จะช่วยยกระดับ ปกป้องและสนับสนุนผู้ปฏิบัติการโทรศัพท์เคลื่อนที่ระบบ GSM ทั่วโลก องค์กรดังกล่าวไม่เป็นเพียงแค่ต่อรองในเรื่องการธุรกิจโทรศัพท์เคลื่อนที่เท่านั้น แต่ยังให้ความสำคัญกับระบบเครือข่ายและการรักษาความปลอดภัยอีกด้วย นอกจากนี้ ยังได้มีการพัฒนาข้อมูลและสนับสนุนกระบวนการที่จะช่วยให้ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ทำงานร่วมกันเพื่อระบุและจัดการกับปัญหาการขายที่ไม่พึงประสงค์ทางข้อความสั้น (SMS spam) โดยมีการตั้งคณะทำงานระหว่างประเทศในเรื่องการขายที่ไม่พึงประสงค์ทางโทรศัพท์เคลื่อนที่ (International working groups on mobile spam) และยังได้ยังได้พัฒนาแนวปฏิบัติที่มิใช่ทางด้านกฎหมาย โดยความร่วมมือของผู้ให้บริการโทรศัพท์เคลื่อนที่ 15 ราย ที่ได้ลงนามร่วมกันในเดือนกุมภาพันธ์ พ.ศ. 2549 ในเดือนกันยายน พ.ศ. 2549

ปลายเดือนกรกฎาคม 2006 สมาคมมีสมาชิกที่เป็นผู้ปฏิบัติการโทรศัพท์เคลื่อนที่จำนวน 699 ราย และเป็นผู้ผลิตและผู้จัดหาวัตถุดิบให้ GSM จำนวน 185 ราย สมาชิกบริหาร ณ ปัจจุบันมาจาก Hutchison Whampoa Group (ฮ่องกง ประเทศจีน), Turkcell Iletisism Hizmetleri (ประเทศตุรกี), Bharti (ประเทศอินเดีย), Roger Communications (ประเทศแคนาดา), Telefonica Moviles (ประเทศสเปน), Singapore Telecommunication, Telenor

Mobile (ประเทศนอรเวย์), SFR (ประเทศฝรั่งเศส), Vodafone (ประเทศอังกฤษ), Orange (ประเทศฝรั่งเศส), Smart (ประเทศฟิลิปปินส์), china Mobile (ประเทศจีน), TeliaSonera (ประเทศสวีเดน), Cingular Wireless (ประเทศสหรัฐอเมริกา), KTF (ประเทศเกาหลี), Orascom Telecom (ประเทศอียิปต์), VimpelCom (ประเทศรัสเซีย), China United Telecommunications (ประเทศจีน) และ NTT DoCoMo (ประเทศญี่ปุ่น) และ T-Mobile International (TIM)

1.3.10 CDMA Development Group (CDG)

กลุ่มนักพัฒนาระบบซีดีเอ็มเอ (CDMA Development Group: CDG) ก่อตั้งเมื่อเดือนตุลาคม พ.ศ.2536 เกิดขึ้นจากการรวมตัวระหว่างประเทศของบริษัทต่างๆที่ร่วมมือกันเพื่อผลักดันให้มีการนำ 3G CDMA wireless systems มาใช้รวมทั้งร่วมส่งเสริมให้มีการพัฒนาเทคโนโลยี 3G CDMA wireless systems อย่างแพร่หลายทั่วโลก ซึ่งกลุ่มนักพัฒนาระบบซีดีเอ็มเอ (CDMA Development Group: CDG) มีองค์กรสมาชิกที่เกี่ยวข้องประกอบด้วยผู้ให้บริการ CDMA (CDMA service providers) ผู้ผลิต (manufacturers) ผู้พัฒนาโปรแกรมคอมพิวเตอร์ (application developers) และผู้ให้บริการเนื้อหา (content providers) ที่ร่วมมือกันช่วยทำให้มั่นใจในขีดความสามารถในการทำงานระหว่างระบบ และช่วยผลักดันให้ผู้บริโภคได้มีโอกาสใช้เทคโนโลยี 3G CDMA ได้เร็วยิ่งขึ้น

1.3.11 Mobile Marketing Association (MMA)[17]

สมาคมการตลาดผ่านโทรศัพท์เคลื่อนที่ (Mobile Marketing Association: MMA) เป็นสมาคมการค้าซึ่งไม่มุ่งหวังผลกำไรที่มีความสำคัญระดับโลก (The premier global non-profit trade association) ตั้งขึ้นเพื่อก่อให้เกิดการพัฒนาตลาดโทรศัพท์เคลื่อนที่ (mobile marketing) และเทคโนโลยีที่เกี่ยวข้อง

สมาคมการตลาดผ่านโทรศัพท์เคลื่อนที่ (Mobile Marketing Association: MMA) เป็น action-oriented organization ที่มุ่งขจัดอุปสรรคต่อการพัฒนาตลาด สร้างคู่มือสื่อโทรศัพท์เคลื่อนที่ (mobile media guidelines) และแนวปฏิบัติที่ดีที่สุดสำหรับสนับสนุนการพัฒนา (best practices for sustainable growth) และกระตุ้นให้มีการใช้ช่องทางโทรศัพท์เคลื่อนที่

---

[17] ดูข้อมูลเพิ่มเติมได้ที่ <www.mmaglobal.com>.

บริษัทสมาชิกมากกว่า 650 บริษัท ทำหน้าที่เป็นตัวแทนในกว่า 40 ประเทศทั่วโลก ซึ่งรวมถึงสมาชิกทุกสมาชิกของ Mobile media ecosystem โดยสำนักงานใหญ่ของสมาคมการตลาดผ่านโทรศัพท์เคลื่อนที่ (Mobile Marketing Association's global headquarters) ตั้งอยู่ในประเทศสหรัฐอเมริกา และในปี พ.ศ.2550 ได้มีการตั้งสาขาในประเทศอเมริกาเหนือ (North America: NA) ยุโรป ตะวันออกกลาง และแอฟริกา (Europe, Middle East & Africa: EMEA) ลาตินอเมริกา (Latin America: LATAM) และเอเชียแปซิฟิค (Asia Pacific: APAC)

2. มาตรการแก้ไขปัญหาที่เกี่ยวกับการทำธุรกรรมผ่านทางโทรศัพท์เคลื่อนที่ในต่างประเทศ

2.1 การคุ้มครองการทำธุรกรรมการค้าผ่านทางโทรศัพท์เคลื่อนที่

2.1.1 การทำธุรกรรมการค้าผ่านทางโทรศัพท์เคลื่อนที่

ประเทศที่ตลาดโทรศัพท์เคลื่อนที่มีการพัฒนาไปมาก ผู้บริโภคมักจะเผชิญกับปัญหาต่างๆ เช่น การได้รับการเสนอขายที่ไม่ได้มีการร้องขอจากผู้ซื้อ และการไม่ได้รับเนื้อหา (Content) ผ่านทางโทรศัพท์เคลื่อนที่ที่ผู้บริโภคสั่งซื้อไป ประเทศเหล่านี้ส่วนใหญ่รับมือกับปัญหาเหล่านี้โดยการใช้กฎหมายทั่วไปว่าด้วยการคุ้มครองผู้บริโภค (General Consumer Protection Act) เช่น กฎหมายว่าด้วยการค้าที่เป็นธรรม (Fair Trade Act) กฎหมายคุ้มครองผู้บริโภค (Consumer Protection Act) หรือกฎหมายว่าด้วยการซื้อขายซึ่งห่างโดยระยะทาง (Distance Sales Act) รวมไปถึงกฎหมายเกี่ยวกับการพาณิชย์ผ่านอุปกรณ์อิเล็กทรอนิกส์ นอกเหนือไปจากการกำกับดูแลตนเอง

ทั้งนี้ บางประเทศได้นำกฎหมายเกี่ยวกับการป้องกันการกระทำที่ไม่เป็นธรรม หรือการกระทำหรือการปฏิบัติที่เป็นการหลอกลวง มาปรับใช้กับการคุ้มครองผู้บริโภคในประเด็นที่เกี่ยวข้องกับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (mobile commerce) ตัวอย่างเช่น กฎหมายว่าด้วยการแข่งขันของประเทศแคนาดา (Canada's Competition Act) อันเป็นบทบัญญัติที่ห้ามมิให้มีการปฏิบัติทางการตลาดที่ก่อให้เกิดความเข้าใจผิดและที่เป็นการหลอกลวง ซึ่งถือเป็นกฎหมายทางเทคโนโลยีที่เป็นกลาง เช่นเดียวกับกฎหมายว่าด้วยข้อปฏิบัติด้านการค้าของประเทศออสเตรเลีย (Australian Trade Practices Act) ก็ถือเป็นกฎหมายเชิงเทคโนโลยีที่เป็นกลาง ซึ่งมีข้อกำหนดที่ปรับใช้อย่างเท่าเทียมกันทั้งในประเด็นการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (mobile commerce issues) และการค้าที่ไม่อยู่ในรูปของโทรศัพท์เคลื่อนที่ (non-mobile forms of

trading) และในประเทศสหรัฐอเมริกาก็ได้นำกฎหมายว่าด้วยการแข่งขันที่ไม่เป็นธรรม (Federal Trade Commission Act: FTC Act) ซึ่งห้ามมิให้มีการกระทำหรือการปฏิบัติที่ไม่เป็นธรรมหรือที่หลอกลวง (unfair or deceptive acts or practices) ในการพาณิชย์ หรือที่กระทบต่อการพาณิชย์มาปรับใช้กับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (mobile commerce) ส่วนในประเทศเยอรมันและสวิสเซอร์แลนด์ ได้นำกฎหมายคุ้มครองผู้บริโภคว่าด้วยสัญญา (Consumer Contract Provisions) มาปรับใช้กับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (mobile commerce) นอกเหนือจากการนำกฎหมายทั่วไปว่าด้วยการคุ้มครองผู้บริโภค (general consumer protection provision) มาปรับใช้แล้ว ประเทศต่างๆ เช่น ออสเตรีย เบลเยี่ยม สาธารณรัฐเช็ก ญี่ปุ่น เกาหลี แมกซิโก โปแลนด์ สาธารณรัฐสโลวัก สวีเดน และอังกฤษ ยังได้นำกฎข้อบังคับว่าด้วยการซื้อขายซึ่งห่างโดยระยะทาง (Distance Sales Regulations) และบทบัญญัติที่มีความเฉพาะเจาะจงมากกว่าในเรื่องการพาณิชย์อิเล็กทรอนิกส์ (electronic commerce) มาปรับใช้ด้วย[18] อีกทั้งคณะกรรมาธิการยุโรป (European Commission) ได้มีรายงานว่าบทบัญญัติว่าด้วยการขายซึ่งห่างโดยระยะทาง (Distance Selling) ใน Directive 97/7/EC[19] ถูกนำมาปรับใช้มากที่สุด ไม่ว่าจะเป็นการกำหนดให้มีข้อกำหนดที่คลอบคลุมก่อนการซื้อขาย การยืนยันข้อมูลต้องมีหลักฐานที่แน่นอน เช่น การยืนยันเป็นลายลักษณ์อักษร ผู้บริโภคมีสิทธิที่จะเลิกสัญญาภายในกำหนดเวลาอย่างน้อย 7 วันทำการโดยไม่ต้องให้เหตุผล และไม่ต้องเสียค่าปรับ นอกจากค่าใช้จ่ายในการส่งคืนสินค้า (สิทธิในการถอนคืน) ทั้งเมื่อยกเลิกสัญญาแล้วผู้บริโภคมีสิทธิจะได้รับเงินคืนภายใน 30 วันนับแต่วันที่ได้ยกเลิก และผู้ขายสินค้าหรือผู้ให้บริการต้องทำการส่งสินค้าหรือให้บริการภายใน 30 วันนับแต่ผู้บริโภคมีคำสั่งซื้อ และคุ้มครองผู้บริโภคจากการขายที่ไม่พึงประสงค์ (unsolicited selling) คุ้มครองจากการใช้บัตรชำระเงินโดยฉ้อโกง (fraudulent use of payment

---

[18] ในกรณีของประเทศเม็กซิโก กฎหมายสหพันธรัฐว่าด้วยการคุ้มครองผู้บริโภค (Federal Law of Consumer Protection: LFPC) ได้ควบคุมธุรกรรมทางการค้าทุกรูปแบบระหว่างผู้ให้บริการและผู้บริโภค ซึ่งรวมถึงการขายทางไกลด้วย ดังนั้น กฎหมายสหพันธรัฐว่าด้วยการคุ้มครองผู้บริโภค (LFPC) สามารถนำไปใช้กับการค้าขายอุปกรณ์สื่อสารเคลื่อนที่ทั่วไป ที่สำคัญการค้าขายทางไกลในเม็กซิโกสามารถควบคุมโดยบทหนึ่งของกฎหมายสหพันธรัฐว่าด้วยการคุ้มครองผู้บริโภค (LFPC) เกี่ยวกับการทำธุรกรรมของผู้บริโภคผ่านอุปกรณ์อิเล็กทรอนิกส์และอุปกรณ์บรรจุข้อมูลด้วยเลเซอร์เช่น แผ่นซีดี (CD) และดีวีดี (DVD)

[19] ดูข้อมูลเพิ่มเติมได้ที่ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:EN:NOT>.

cards) ความไม่สมบูรณ์ของการสละสิทธิหรือหน้าที่ไม่ว่ากระทำโดยผู้บริโภค หรือผู้ให้บริการ ย่อมอยู่ภายใต้ข้อกำหนดใน Directive [20] อีกทั้ง พระราชบัญญัติว่าด้วยการประกอบกิจการโทรคมนาคม (Telecommunication Act) ยังนำมาใช้ควบคุมคุณภาพของการให้บริการผ่านทางโทรศัพท์เคลื่อนที่ เช่นในประเทศเยอรมัน[21] และโปแลนด์

2.1.2 การขายที่ไม่ได้ขอให้ส่งมา และการไม่ได้รับสินค้า หรือการดาว์นโหลดที่ไม่สมบูรณ์

การขายที่ไม่ได้ขอให้ส่งมา (Unsolicited sales)

บางประเทศได้มีความกระตือรือร้นที่จะนำบทบัญญัติในพระราชบัญญัติว่าด้วยการคุ้มครองผู้บริโภค (consumer protection act) ที่มีอยู่มาปรับใช้กับอาชญากรรมที่เกี่ยวพันกับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (mobile commerce) ในกรณีการขายเนื้อหาทางโทรศัพท์เคลื่อนที่ (Mobile Content) ผ่านทางโทรศัพท์เคลื่อนที่ที่ไม่พึงประสงค์ในประเทศเยอรมันนั้น ตามมาตรา 241a แห่งประมวลกฎหมายแพ่งและพาณิชย์ของเยอรมัน (BGB) ได้คุ้มครองผู้บริโภคจากการได้รับสินค้าหรือบริการที่ไม่ได้สั่งซื้อ ในประเทศเบลเยี่ยม พระราชบัญญัติว่าด้วยการคุ้มครองผู้บริโภคได้มีการปรับให้เข้ากับแนวปฏิบัติชนิดนี้เป็น “*achat forcé*”[22] ส่วนแนวปฏิบัติว่าด้วยการค้าที่ไม่เป็นธรรมของคณะกรรมาธิการยุโรป (European Commission’s Unfair Commercial Practices) ใน Directive (2005/29/EC) ก็ครอบคลุมถึงการขายเนื้อหาทางโทรศัพท์เคลื่อนที่ (Mobile Content) ผ่านทางโทรศัพท์เคลื่อนที่ที่ไม่พึงประสงค์

การไม่ได้รับสินค้า (Non-delivery) หรือการดาว์นโหลดที่ไม่สมบูรณ์ (Incomplete download)

ในบางครั้งผู้บริโภคอาจจะไม่ได้รับสินค้าที่สั่งซื้อผ่านทางโทรศัพท์เคลื่อนที่ หรือถูกเรียกเก็บเงินค่าบริการเนื้อหาทางโทรศัพท์เคลื่อนที่ (Mobile Content) ซึ่งดาว์นโหลดไม่สมบูรณ์

---

[20] ดูข้อมูลเพิ่มเติมได้ที่ <http://ec.europa.eu/consumers/cons_int/safe_shop/dist_sell/index_en.htm>.

[21] ดูข้อมูลเพิ่มเติมได้ที่ <http://www.iuscomp.org/gla/statutes/TKG.htm>.

[22] ข้อ 76 แห่งกฎหมายลงวันที่ 14 กรกฎาคม พ.ศ. 2534 ในแนวปฏิบัติว่าด้วยการค้าและข้อมูลและการคุ้มครองผู้บริโภค (The practices of trade and information and consumer protection: LPC).

มาตรการหลักในกรณีนี้คือแผนการเจรจาประนีประนอม ในประเทศเกาหลี ยกตัวอย่างเช่น ตามกฎหมายว่าด้วยการคุ้มครองผู้บริโภคในการพาณิชย์อิเล็กทรอนิกส์ (Consumer Protection in Electronic Commerce: CPEC) บังคับให้ผู้ประกอบธุรกิจต้องส่งสินค้าภายใน 3 วันทำการนับจากที่ได้รับการชำระเงินจากผู้บริโภค หรือต้องคืนเงินภายใน 3 วัน ในประเทศสหรัฐอเมริกานั้นอาจนำกฎข้อบังคับว่าด้วยการสั่งซื้อสินค้าทางไปรษณีย์หรือโทรศัพท์ของคณะกรรมาธิการการค้าแห่งสหพันธรัฐ (Federal Trade Commission's Mail or Telephone Order Merchandise Rule) มาปรับใช้กับการการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ โดยกฎระเบียบดังกล่าวได้กำหนดให้ผู้ประกอบธุรกิจต้องกล่าวชี้แจงหรือบอกเป็นนัยถึงหลักเกณฑ์ที่สมเหตุสมผลว่าสามารถที่จะส่งให้ภายในเวลาที่แน่นอน

<u>การกำกับดูแลตนเอง และความร่วมมือในการกำกับดูแล</u>

ในประเทศสมาชิกหลายๆประเทศซึ่งรวมถึงประเทศออสเตรเลีย ออสเตรีย แคนาดา เดนมาร์ก ฟินแลนด์ เกาหลี นอรเวย์ สวีเดน อังกฤษ และสหรัฐอเมริกา ประมวลกฎหมายต่างๆว่าด้วยการกำกับดูแลตนเอง หรือความร่วมมือในการกำกับดูแล หรือแผนการอื่นๆได้ถูกพัฒนาโดยอุตสาหกรรม ตัวอย่างเช่น ในประเทศสหรัฐอเมริกา สมาคมการตลาดผ่านโทรศัพท์เคลื่อนที่ (Mobile Marketing Association: MMA) ได้รับเอาหลักเกณฑ์ 5 ข้อ[23]ในแนวปฏิบัติว่าด้วยการซื้อ

---

[23] แนวปฏิบัติว่าด้วยการซื้อขายสินค้าหรือบริการทางโทรศัพท์เคลื่อนที่ (Code of conduct for mobile marketing) มีหลักเกณฑ์ 5 ข้อ ประกอบไปด้วย

1) หลักการแจ้ง (Notice) ที่ผู้ซื้อขายในตลาดทางโทรศัพท์เคลื่อนที่ (Mobile Marketers) ต้องมีการแจ้ง (Notice) อธิบายข้อกำหนดและเงื่อนไขของรายการซื้อขาย (marketing program) ต่อผู้ใช้บริการที่เข้าใจง่าย และสามารถพบได้อย่างรวดเร็ว ซึ่งการแจ้งดังกล่าวควรรวมถึงข้อมูลที่เพียงพอที่จะให้ผู้ใช้บริการทำการตัดสินใจเกี่ยวกับทางเลือกว่าข้อมูลนั้นจะถูกใช้สำหรับเป็นรายการการซื้อขายอย่างไร อันเป็นหลักการเบื้องต้นของจรรยาบรรณทางธุรกิจว่าด้วยข้อมูลส่วนบุคคลของสมาคมการตลาดผ่านโทรศัพท์เคลื่อนที่ (MMA privacy Code of Conduct)

2) หลักทางเลือกและความยินยอม (Choice & Consent) นักการตลาดทางโทรศัพท์เคลื่อนที่ (Mobile Marketers) เคารพสิทธิของผู้ใช้บริการในการควบคุมข้อความทางโทรศัพท์เคลื่อนที่ที่พวกเขาได้รับ โดยให้นักการตลาดทางโทรศัพท์เคลื่อนที่ (Mobile Marketers) ขอและได้รับความยินยอม โดยการได้รับอนุญาตโดยชัดแจ้ง (explicit opt-in) จากผู้ใช้บริการสำหรับการส่งข้อความทางโทรศัพท์เคลื่อนที่ทุกรายการ ซึ่งการขอและได้รับความยินยอมนี้

สามารถทำผ่านกระบวนการอนุญาต (opt-in) ทางข้อความสั้น (SMS) ข้อความมัลติมีเดีย (MMS) เสียงตอบรับ (voice response) การลงทะเบียนทางเว็บไซต์ (website registration) หรือวิธีการอื่นที่ MMA ยอมรับหรือที่ถูกต้องตามกฎหมาย นอกจากนี้ นักการตลาดทางโทรศัพท์เคลื่อนที่ (Mobile Marketers) ต้องจัดให้มีกระบวนการปฏิเสธ (opt-out) ที่ง่าย เพื่อให้ผู้ใช้บริการสามารถยุติการรับข้อความ และต้องให้ผู้ใช้บริการสามารถเลือกที่จะปฏิเสธ (opt-out) ได้ทุกข้อความ ทั้งนี้ การปฏิเสธ (opt-out) จะต้องสามารถนำไปใช้ประโยชน์ได้เช่นเดียวกับวิธีการที่ใช้ในการได้รับอนุญาต (opt-in) และจะต้องสามารถพบได้ง่ายโดยผู้ใช้

3) หลักรูปแบบการให้บริการและข้อจำกัด (Customization & Constraint)

หลักรูปแบบการให้บริการ (Customization) นักการตลาดทางโทรศัพท์เคลื่อนที่ (Mobile Marketers) ทำให้แน่ใจว่าได้สะท้อนให้เห็นถึงความคาดหวังของผู้บริโภคทั่วโลกที่สามารถนำไปปรับใช้ได้ในทุกตลาด (national marketplace) การตลาดผ่านช่องทางทางโทรศัพท์เคลื่อนที่เป็นวิธีที่ได้ผลดีที่สุดเมื่อส่งไปยังเป้าหมายที่เหมาะสม และข้อมูลของผู้ใช้บริการที่ถูกเก็บเพื่อวัตถุประสงค์ทางการตลาดควรจะใช้เฉพาะงาน อย่างการตลาดเมื่อปรากฏความสนใจของผู้ใช้บริการ

หลักข้อจำกัด (Constraint) นักการตลาดทางโทรศัพท์เคลื่อนที่ (Mobile Marketers) ควรตั้งเป้าหมายและจำกัดข้อความทางโทรศัพท์เคลื่อนที่ที่ผู้ใช้บริการร้องขอ ข้อความทางโทรศัพท์เคลื่อนที่ควรจัดให้มี value ต่อผู้ใช้บริการ ซึ่ง value อาจจะส่งในหลายวิธี รวมถึงการส่งเสริมสินค้าและบริการ (product and service enhancements) การเตือน (reminders) การแจกรางวัล (sweepstakes) การแข่งขัน (contests) การขอข้อมูล (requested information) ความบันเทิง (entertainment) หรือส่วนลด (discounts)

4) หลักการรักษาความปลอดภัย (Security) นักการตลาดทางโทรศัพท์เคลื่อนที่ (Mobile Marketers) ต้องนำทฤษฎีที่สมเหตุสมผล กระบวนการจัดการ และการดำเนินงานที่เป็นรูปธรรมมาปรับใช้ในการคุ้มครองข้อมูลของผู้ใช้บริการที่ถูกเก็บไว้เพื่อใช้ในการทำรายการทางการตลาดต่างๆทางโทรศัพท์เคลื่อนที่ จากการใช้โดยไม่มีอำนาจ (unauthorized use) การปรับแต่ง (alteration) การเปิดเผย (disclosure) การกระจาย (distribution) หรือการเข้าถึง (access)

5) หลักการบังคับใช้และความสามารถในการชี้แจงหรือให้เหตุผลได้ (Enforcement & Accountability) นักการตลาดทางโทรศัพท์เคลื่อนที่ (Mobile Marketers) คาดว่าสมาชิกจะปฏิบัติตาม MMA Global Code of Conduct และมีการรวมมาตรการ (Code) ไว้ในคู่มือต่างๆของ MMA ที่สามารถนำไปปรับใช้ได้ (applicable MMA Guidelines) ดังที่ได้นำมาใช้กับนักการตลาด

ขายสินค้าหรือบริการทางโทรศัพท์เคลื่อนที่ (Code of conduct for mobile marketing)[24] หนึ่งในนั้นคือผู้บริโภคจะต้องเลือกให้ความยินยอมกับทุกรายการการส่งข้อความทางโทรศัพท์เคลื่อนที่ (mobile messaging programs) ที่จะได้รับและ/หรือถูกเสนอบริการ เพื่อที่จะหลีกเลี่ยงการเสนอขายที่ไม่พึงประสงค์

ทางโทรศัพท์เคลื่อนที่ (Mobile Marketers) ทั่วโลก รวมถึง MMA Consumer Best Practices (CBP) Guidelines ที่สามารถปรับใช้กับ certain national markets

ก่อนจะถึงเวลาที่มาตรการ (Code) สามารถบังคับใช้ได้อย่างมีประสิทธิภาพโดยองค์กรในการบังคับใช้ฝ่ายที่สาม (third party enforcement organization) นักการตลาดทางโทรศัพท์เคลื่อนที่ (Mobile Marketers) หวังที่จะใช้การประเมินผลการปฏิบัติของพวกเขาเพื่อรับรองการยอมปฏิบัติตามมาตรการ (Code)

ดูข้อมูลเพิ่มเติมได้ที่ <http://www.mmaglobal.com/policies/code-of-conduct>.

[24] นอกจากนี้ ในเดือนพฤษภาคม พ.ศ. 2548 สมาคมการตลาดผ่านโทรศัพท์เคลื่อนที่ (Mobile Marketing Association: MMA) ได้ร่วมมือกับสมาคมการสื่อสารระบบเซลลูลาร์และอินเตอร์เน็ต (Cellular Telecommunications and Internet Association: CTIA) พัฒนา “คู่มือแนวปฏิบัติอันเป็นเลิศสำหรับการให้บริการข้อมูลผ่านอุปกรณ์สื่อสารเคลื่อนที่” (Best Practices Guidelines for Cross-Carrier Mobile Content Services) ซึ่งครอบคลุมในส่วนของการโฆษณาและการวางแผนการขายพิเศษ, ดูข้อมูลเพิ่มเติมได้ที่
<www.mmaglobal.com/bestpractices.pdf>

และสมาคมการสื่อสารระบบเซลลูลาร์และอินเตอร์เน็ต (Cellular Telecommunications and Internet Association: CTIA) ยังมีกฎหมายคุ้มครองผู้บริโภคว่าด้วยบริการไร้สาย (Consumer Code for Wireless Service) ด้วย ดูข้อมูลเพิ่มเติมได้ที่ <files.ctia.org/pdf/The_Code.pdf>.

ในประเทศแคนาดา[25]และเดนมาร์ก[26]ภาคอุตสาหกรรมได้เป็นผู้นำในการริเริ่มนำการกำกับดูแลตนเองมาใช้สำหรับบริการข้อมูลเสริมพิเศษ (Premium Content) ต่างๆผ่านทางโทรศัพท์เคลื่อนที่ อีกทั้ง ในประเทศออสเตรเลียก็กำลังพัฒนาขอบข่ายการกำกับดูแลตนเองที่ครอบคลุมมากขึ้นสำหรับบริการเสริมพิเศษทางโทรศัพท์เคลื่อนที่ต่างๆ คณะกรรมการกิจการโทรคมนาคมแห่งชาติประเทศออสเตรเลีย (Australian Communications Authority: ACA) ซึ่งในปัจจุบันเป็นส่วนของคณะกรรมการกิจการโทรคมนาคมและสื่อมวลชนแห่งชาติประเทศออสเตรเลีย (Australian Communication and Media Authority: ACMA) ได้จัดทำข้อตกลงในเดือนมิถุนายน พ.ศ. 2548 ซึ่งเสนอกฎระเบียบสำหรับบริการต่างๆเหล่านี้ และส่งเสริมภาคอุตสาหกรรมในการพัฒนาแผนการกำกับดูแลตนเอง[27] ซึ่งแผนการกำกับดูแลตนเองสำหรับบริการข้อมูลเสริมพิเศษในโทรศัพท์เคลื่อนที่ (Mobile Premium Services Self-Regulatory Scheme) เคยพัฒนาและได้รับการอนุมัติโดยคณะกรรมการกิจการโทรคมนาคมและสื่อมวลชนแห่งชาติประเทศออสเตรเลีย (Australian Communication and Media Authority: ACMA) ในวันที่ 28 กันยายน พ.ศ. 2549[28] ผู้ให้บริการส่งข้อมูล (Carriage service providers) และผู้ให้บริการเนื้อหา (Content service providers) ที่ไม่ได้เป็นสมาชิกของคณะกรรมการกิจการโทรคมนาคมและสื่อมวลชนแห่งชาติประเทศออสเตรเลีย (Australian Communication and

---

[25] ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ของแคนาดา (Canadian mobile carriers) กับสมาคมโทรคมนาคมไร้สายแคนาดา (Canadian Wireless Telecommunications Association: CWTA) มีความคิดริเริ่มที่จะนำบทสรุปข้อปฏิบัติทั่วไป (Common short code code of conduct) มาใช้, ดูข้อมูลเพิ่มเติมได้ที่ <www.txt.ca/common.htm>.

[26] สมาคมอุตสาหกรรมโทรคมนาคม (Telecommunication Industries Association) ประเทศเดนมาร์กมีกรอบความตกลงว่าด้วยการให้บริการข้อมูลทางโทรศัพท์เคลื่อนที่, ดูข้อมูลเพิ่มเติมได้ที่ <www.teleindu.dk/t2w_358.asp>.

[27] ส่วนที่ 5 ของบทสรุปของผู้ให้บริการโทรคมนาคม (บริการเสริมพิเศษทางโทรศัพท์เคลื่อนที่) พ.ศ. 2548 (Telecommunications Service Provider (Mobile Premium Services) Determination 2005) ฉบับที่ 1, ดูข้อมูลเพิ่มเติมได้ที่ <www.acma.gov.au/acmainterwr/_assets/main/lib100039/mobile%20premium%20services%20determination%2029june05.pdf>.

[28] ดูข้อมูลเพิ่มเติมเกี่ยวกับแผนการดังกล่าวได้ที่ <www.commsalliance.com.au/projects/mobile_premium_services>.

Media Authority: ACMA) ซึ่งยอมรับต่อแผนการการกำกับดูแลตนเอง ต่างผูกพันโดยแผนการดังกล่าวไปโดยอัตโนมัติ ซึ่งแผนการดังกล่าวได้รับการปรับปรุงใน June 2005 determination ทั้งสองแผนการดังกล่าวจะมีผลบังคับใช้ในวันที่ 29 ตุลาคม พ.ศ. 2549

2.1.3 การให้บริการข้ามพรมแดน

ในคำแถลงการณ์ของสหภาพยุโรปและเขตเศรษฐกิจยุโรป (European Economic Area: EEA) สมาคมการค้าเสรียุโรป (European Free Trade Association: EFTA) กรณีการให้บริการข้ามพรมแดนนั้นจะปฏิบัติตามหลักการที่ปรากฏใน Injunctions Directive[29] ในประเทศแถบสแกนดิเนเวียกฎระเบียบพื้นฐานมีอยู่ในแถลงการณ์สถานะ (ตุลาคม 2545) ของผู้รับคำร้องผู้บริโภคสแกนดิเนเวียด้านพาณิชย์อิเล็กทรอนิกส์ (E-commerce) และการตลาดบนอินเตอร์เน็ตจะสามารถนำไปใช้ได้กับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ กลุ่มประเทศเหล่านี้ยังได้ยอมรับแถลงการณ์สถานะร่วมว่าด้วยเรื่องบริการเนื้อหาทางโทรศัพท์เคลื่อนที่ (Mobile content services) ในเดือนมีนาคม พ.ศ. 2549[30] แต่ในทางกลับกันกรณีการขายไม่พึงประสงค์ การให้ข้อมูลที่ไม่ตรงกับความจริงและข้อความที่ไม่พึงประสงค์ (SMS spam) นั้นในประเทศญี่ปุ่นได้นำกฎหมายเฉพาะว่าด้วยธุรกรรมทางการค้า (Specified Commercial Transactions Law) มาปรับใช้เฉพาะกรณีที่ทั้งผู้ขายและผู้บริโภคต่างอยู่ในเขตอำนาจศาลญี่ปุ่น

2.1.4 การชำระเงิน

คณะกรรมาธิการยุโรป (European commission) ได้มีการพิจารณาว่า เฉพาะผู้ให้บริการชำระเงินทางโทรศัพท์เคลื่อนที่ที่ถ่ายโอนมูลค่าเงิน (monetary value) โดยตรงจากอุปกรณ์โทรศัพท์เคลื่อนที่ (handset) ไปยังร้านค้าเท่านั้น ที่จะจำกัดความว่าเป็นเงินอิเล็กทรอนิกส์ (e-money) และตกอยู่ภายใต้ e-Money Directive ซึ่งการชำระเงินผ่านทางโทรศัพท์เคลื่อนที่ส่วนใหญ่ทำโดยอ้อม ที่เป็นการชำระเงินโดยโอนผ่านธนาคาร ดังนั้น บริการการชำระเงินผ่านทางโทรศัพท์เคลื่อนที่โดยส่วนใหญ่แล้วจะไม่ตกอยู่ในขอบเขตของ e-Money Directive แต่แม้กระทั่งบริการที่อยู่ในคำจำกัดความก็อาจไม่อยู่ในขอบเขตของ e-Money Directive เพื่อหลีกเลี่ยงการ

---

[29] หมายถึง Directive 98/27/EC of the European Parliament and of the Council of 19th May 1998 on injunctions for the protection of consumers' interests.

[30] ตัวอย่างเช่นใน <www.forbrukerombudet.no/asset/2305/1/2305_1.pdf> (ภาษานอรเวย์).

บังคับใช้ e-Money Directive กับบริการที่มีความเสี่ยงต่ำและมีมูลค่าที่เกี่ยวข้องต่ำเมื่อเปรียบเทียบกับค่าธรรมเนียมที่เรียกเก็บสำหรับบริการติดต่อสื่อสารตามปกติ อย่างไรก็ตาม ไม่ว่าจะเป็นการชำระเงินล่วงหน้า (pre-payment) ซึ่งอยู่ภายใต้ Directive on e-Money (Directive 2000/46/EC) หรือชำระเงินแบบเรียกเก็บภายหลัง (post-payment) ตามกรอบกฎหมายใหม่ (proposed new framework) ข้อกำหนดที่ควบคุมในการคุ้มครองผู้ใช้บริการก็มีความเสี่ยง เพราะหากเพิ่มข้อกำหนดที่เข้มงวดมากขึ้นก็จะทำให้ตลาดไม่ก้าวหน้า[31]

ทั้งนี้ ในสหภาพยุโรป (Directive 2000/46/EC) มีหลักเกณฑ์ในการคุ้มครองผู้บริโภคเพื่อรับรองความเชื่อมั่นของผู้ถือเงินอิเล็กทรอนิกส์อยู่หลายประการ กล่าวคือ การรับแลกเปลี่ยนเงินอิเล็กทรอนิกส์คืนเป็นเงินสด (Article 5: Redeemability) ผู้ออกเงินอิเล็กทรอนิกส์มีหน้าที่ในการรับแลกเปลี่ยนเงินอิเล็กทรอนิกส์คืนเป็นเงินตราที่ออกโดยรัฐบาลกลาง ในรูปของเหรียญธนบัตร หรือโดยการโอนเข้าบัญชีของผู้ถือเงินอิเล็กทรอนิกส์ตามยอดเงินอิเล็กทรอนิกส์คงเหลือในอุปกรณ์อิเล็กทรอนิกส์ ในกรณีที่ผู้ถือเงินอิเล็กทรอนิกส์เรียกร้องในระหว่างที่เงินอิเล็กทรอนิกส์ยังคงใช้งานได้ (ไม่หมดอายุ) โดยต้องไม่มีค่าธรรมเนียมในการแลกคืน เว้นแต่ค่าธรรมเนียมที่มีความจำเป็นในการดำเนินการคืนเงิน เช่น ค่าธรรมเนียมในการโอนเงินเข้าบัญชีของผู้ถือเงินอิเล็กทรอนิกส์ เป็นต้น สัญญาระหว่างผู้ออกเงินอิเล็กทรอนิกส์ และผู้ถือเงินอิเล็กทรอนิกส์จะต้องแสดงเงื่อนไขในการแลกคืนเงินอิเล็กทรอนิกส์เป็นเงินสดเอาไว้ในสัญญาอย่างชัดแจ้ง โดยในสัญญาอาจระบุเงื่อนไขขั้นต่ำสำหรับการแลกคืนเงินสด ทั้งนี้ ในกรณีที่เงินอิเล็กทรอนิกส์ที่อยู่ในความครอบครองของผู้ถือยังใช้ไม่หมด หรือเงินอิเล็กทรอนิกส์ไม่สามารถใช้การได้ เนื่องจากไม่มีร้านค้าใดให้การยอมรับ ผู้ถือเงินอิเล็กทรอนิกส์สามารถส่งเงินอิเล็กทรอนิกส์กลับคืนไปยังผู้ออกเงินอิเล็กทรอนิกส์เพื่อแลกเปลี่ยนคืนเป็นเงินตราที่ออกโดยรัฐบาลกลางได้

การที่ผู้ออกเงินอิเล็กทรอนิกส์นำเงินของลูกค้าไปลงทุนเพื่อแสวงหาผลกำไรให้แก่กิจการอาจก่อให้เกิดความเสี่ยงกับผู้ถือเงินอิเล็กทรอนิกส์ เนื่องจากเงินที่อยู่ในความครอบครองของผู้ออกเงินอิเล็กทรอนิกส์แท้จริงเป็นเงินของผู้ถือเงินอิเล็กทรอนิกส์ ดังนั้น จึงให้มีการจำกัดการลงทุนของสถาบันผู้ออกเงินอิเล็กทรอนิกส์ (Electronic Money Institution) โดยจะต้องเป็นการลงทุนในทรัพย์สินที่มีสภาพคล่องสูง และมีความเสี่ยงต่ำเท่านั้น (Article 5 (1)-(6)) และการลงทุน

---

[31] Viviane Reding, "Towards a European Payment and Information Space: m-Payments", Roundtable Conference on m-Payments, (Brussels, June 29, 2006).

ในแต่ละประเภทต้องได้รับการพิจารณาจากเจ้าพนักงานผู้มีอำนาจ[32] นอกจากนี้ ผู้ออกเงินอิเล็กทรอนิกส์ต้องเตรียมเงินสำหรับการไถ่ถอนมูลค่าเงินอิเล็กทรอนิกส์ไว้ตลอดเวลา

นอกจากนี้ ใน Article 7 กำหนดให้ผู้ออกเงินอิเล็กทรอนิกส์ต้องมีระบบจัดการที่มั่นคง และรอบคอบ และมีกระบวนการในการบริหาร การทำบัญชี รวมถึงจะต้องมีกลไกในการควบคุมภายในอย่างเพียงพอ โดยระบบในการบริหารจัดการควรที่จะตอบสนองต่อความเสี่ยงทางการเงิน และความเสี่ยงอย่างอื่นที่อาจส่งผลกระทบต่อสถาบันผู้ออกเงินอิเล็กทรอนิกส์ เช่น ความเสี่ยงทางด้านการดำเนินการ ความเสี่ยงทางด้านเทคนิค และความเสี่ยงที่เกี่ยวเนื่องกับนิติบุคคลอื่นๆที่มีส่วนร่วมในการออกเงินอิเล็กทรอนิกส์ และทำหน้าที่เกี่ยวเนื่องใกล้ชิดกับการดำเนินธุรกิจของสถาบันผู้ออกเงินอิเล็กทรอนิกส์

ในการควบคุมภายในสถาบันผู้ออกเงินอิเล็กทรอนิกส์ และการบริหารจัดการที่ตอบสนองความเสี่ยงทางด้านเทคนิค และความเสี่ยงที่เกิดจากพนักงาน ตัวแทน หรือบุคคลอื่นที่มีส่วนร่วม หรือมีหน้าที่เกี่ยวเนื่องกับการออกเงินอิเล็กทรอนิกส์ เพื่อเป็นกรอบแนวทางในการที่ประเทศสมาชิกจะนำไปบัญญัติเป็นกฎหมายภายใน โดยในประเทศอังกฤษ The Financial Services and Market Act 2000: FSMA ได้กำหนดให้ผู้ออกเงินอิเล็กทรอนิกส์จะต้องดูแลระบบและการควบคุมภายในองค์กรให้มีความเหมาะสมกับธุรกิจของตน และต้องกำหนดหน้าที่ของตัวแทน หรือบุคคลภายนอกที่เป็นคู่สัญญาในการดำเนินการออกเงินอิเล็กทรอนิกส์กับผู้ออกเงินอิเล็กทรอนิกส์ และผู้ออกเงินอิเล็กทรอนิกส์ต้องรับรองว่าธุรกรรมเงินอิเล็กทรอนิกส์จะไม่ล้มเหลวหรือตีกลับ และจะต้องให้การรับรองว่ามีมาตรการในการดูแลรักษาฐานข้อมูลเกี่ยวกับธุรกรรมเงินอิเล็กทรอนิกส์ เพื่อให้มีความสมบูรณ์กับคู่สัญญาทุกฝ่าย และมีการเก็บบันทึกข้อมูลเกี่ยวกับธุรกรรมเงินอิเล็กทรอนิกส์ นอกจากนี้ สถาบันผู้ออกเงินอิเล็กทรอนิกส์ต้องคัดเลือกบุคคลที่มีความเหมาะสมในการปฏิบัติหน้าที่ในสถาบันผู้ออกเงินอิเล็กทรอนิกส์ โดยบุคคลที่จะเข้ามาบริหารจัดการ หรือปฏิบัติงานในสถาบันผู้ออกเงินอิเล็กทรอนิกส์จะต้องมีความซื่อสัตย์ มีชื่อเสียง และมีฐานะการเงินมั่นคง ในกรณีที่สถาบันเงินอิเล็กทรอนิกส์ฝ่าฝืนกฎหมายนี้ FSA มีอำนาจเพิกถอนหรือเปลี่ยนแปลงการอนุญาตให้ประกอบธุรกิจเงินอิเล็กทรอนิกส์ หรือใช้มาตรการลงโทษได้

---

[32] Rolf H.Weber, “EC E-Money Directive Background, Problems and Prospective,”The London Institute of international Banking, Finance and Development Law Ltd, p.18.

2.1.5 การโฆษณา

กฎหมายคุ้มครองผู้บริโภคของออสเตรเลีย บัญญัติไว้ในส่วนที่ 5 ของพระราชบัญญัติการปฏิบัติทางการค้า ค.ศ. 1947 (The Trade Practices Act 1974: TPA)[33] โดยกำหนดว่า ผู้ประกอบการจะต้องไม่ดำเนินการในทางการค้าหรือการพาณิชย์ ซึ่งก่อให้เกิดความเข้าใจผิดหรือหลอกลวง หรือซึ่งอาจก่อให้เกิดความเข้าใจผิดหรือหลอกลวง[34] นอกจากนี้ การนิ่งเงียบไม่เปิดเผยข้อความจริงที่ปรากฏในข้อความโฆษณาอาจเป็นการก่อให้เกิดความเข้าใจผิดในสาระสำคัญของสินค้าและบริการได้เช่นกันหากว่าผู้โฆษณามีหน้าที่ต้องเปิดเผยข้อความจริงเช่นว่านั้น ซึ่งมาจากพื้นฐานแนวความคิดเรื่องการคุ้มครองผู้บริโภคที่ว่า ผู้ผลิตสินค้าหรือผู้ให้บริการจะต้องรับผิดอย่างเคร่งครัด (Strict liability) เพราะความชำรุดบกพร่องต่างๆของสินค้าหรือบริการที่เกิดขึ้นทั้งหมด ถือว่าอยู่ในความดูแลรับผิดชอบของผู้ผลิตหรือผู้ให้บริการ เพราะเป็นผู้ที่มีความรู้ในสินค้าหรือบริการของตนมากกว่าผู้บริโภค ดังนั้น จึงมีหน้าที่ต้องเปิดเผยข้อความจริงเกี่ยวกับสินค้าหรือบริการให้ครบถ้วนสมบูรณ์ เพื่อมิให้ผู้บริโภคเกิดความเข้าใจผิดพลาดในสินค้าหรือบริการนั้นๆ ทั้งนี้ หลักผู้ซื้อต้องระวัง (*Caveat Emptor*) จะถูกปฏิเสธโดยศาลอย่างสิ้นเชิง เนื่องจากผู้ซื้อไม่อยู่ในฐานะที่จะตรวจสอบสินค้าหรือบริการได้ดีไปกว่าตัวผู้ผลิตสินค้าหรือผู้ให้บริการเอง[35] นอกจากนั้น การกระทำความผิดตามมาตรา 52 ผู้กระทำผิดได้รับเพียงโทษทางแพ่งเท่านั้น เจตนาภายในจิตใจจึงมิใช่องค์ประกอบสำคัญ ผู้โฆษณาจึงไม่อาจอ้างได้[36] และ

---

[33] บทบัญญัติที่เกี่ยวข้องกับข้อความโฆษณาที่จะก่อให้เกิดความเข้าใจผิดแก่ผู้บริโภคนี้ ได้แก่ มาตรา 52 มาตรา 53 มาตรา 53A มาตรา 55 มาตรา 55A มาตรา 56 และมาตรา 59.

[34] มาตรา 52 “A corporation shall not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive”.

[35] Ray Steinwall, ‘Part V – Consumer Protection’ Annotated Trade Practices Act 1974, 2001 ed., Sydney, Butterworths, 2001, p. 211.

[36] Russel V Miller, ‘Part V: Consumer Protection’ *Millers's Annotated Trade Practices Act*, 22nd ed., Sydney, LBC Information Services, 2001, p. 374.

โฆษณาที่จะก่อให้เกิดความเข้าใจผิด ผู้กระทำผิดต้องรับโทษอาญา[37]ด้วยตามมาตรา 53 ซึ่งเป็นความผิดเฉพาะ และอาจต้องรับโทษทางแพ่งตามมาตรา 52 ซึ่งเป็นบททั่วไปด้วย

2.2 การเปิดเผยข้อมูลในกรณีหน้าจอขนาดเล็ก

มาตรการทางกฎหมายที่ใช้คุ้มครองในกรณีความไม่เพียงพอในการเปิดเผยข้อมูล

โดยทั่วไปกฎหมายคุ้มครองผู้บริโภคกำหนดให้ผู้ประกอบธุรกิจต้องจัดให้มีข้อมูลเกี่ยวกับการทำธุรกรรมทางการค้าในทางที่ชัดเจนและที่เข้าใจได้ ในออสเตรเลีย การไม่สามารถเปิดเผยหรือเปิดเผยไม่เพียงพอสามารถรวมอยู่ภายใต้หัวข้อ การจัดการการกระทำที่ก่อให้เกิดความเข้าใจผิดและหลอกลวง (misleading and deceptive conduct) ของพระราชบัญญัติระเบียบว่าด้วยการค้า ในแมกซิโกนั้นมีกฎหมายสหพันธรัฐว่าด้วยการคุ้มครองผู้บริโภค (Federal Law of Consumer Protection: LFPC) ที่กำหนดให้ผู้ประกอบธุรกิจจะต้องจัดให้มีข้อมูลที่ถูกต้องที่สามารถตรวจสอบได้ เพื่อไม่ให้เกิดความเข้าใจผิด หรือเกิดการใช้ที่ผิดพลาด (หมวด 3 มาตรา 32) ทั้งยังต้องจัดให้มียอดรวมที่จะเรียกเก็บเงิน (มาตรา 7ทวิ) ที่อยู่ทางไปรษณีย์ หมายเลขโทรศัพท์ และข้อมูลอื่นๆที่เกี่ยวข้อง เช่น ข้อกำหนดและเงื่อนไขต่างๆ ค่าใช้จ่าย ค่าใช้จ่ายที่จะเรียกเก็บเพิ่มเติม และรูปแบบการชำระเงินต่างๆ (มาตรา 76ทวิ) นอกเหนือจากนั้น กฎหมายสหพันธรัฐว่าด้วยการคุ้มครองผู้บริโภค (Federal Law of Consumer Protection: LFPC) (มาตรา 57) ยังกำหนดให้ผู้ให้บริการต้องแสดงค่าธรรมเนียมต่างๆอย่างเปิดเผย

พระราชบัญญัติว่าด้วยการคุ้มครองผู้บริโภคประเทศฟินแลนด์ (Finnish Consumer Protection Act) กำหนดให้ผู้ประกอบธุรกิจต้องจัดเตรียมข้อมูลให้แก่ลูกค้าในทางที่เหมาะสมเพื่อให้เข้าใจวิธีการใช้งานที่เป็นการติดต่อสื่อสารระยะไกล (หมวด 6 มาตรา 13 การขายตรงตามบ้าน (Door-to-door selling) และการขายซึ่งห่างโดยระยะทาง (Distance selling)) ในกรณีของการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (mobile commerce) ความยืดหยุ่นก็เป็นส่งที่จำเป็นเพราะความจุที่จำกัดของหน้าจอขนาดเล็กอาจทำให้ไม่สามารถที่จะจัดให้มีรายละเอียดทุกอย่างในข้อความ (text message) ได้ อย่างไรก็ตาม กลุ่มพิทักษ์สิทธิผู้บริโภคแห่งฟินแลนด์ (Finnish Consumer Ombudsman) พิจารณาว่าเพียงแค่ให้ที่อยู่ทางอินเตอร์เน็ต (Internet address) ใน

---

[37] ตามมาตรา 79 และมาตรา 79A แห่งพระราชบัญญัติการปฏิบัติทางการค้า ค.ศ. 1947 โทษทางอาญาได้แก่ โทษปรับ และโทษจำคุก ในกรณีบุคคลธรรมดาปรับไม่เกิน 40,000 ดอลลาร์ และในกรณีนิติบุคคลปรับไม่เกิน 200,000 ดอลลาร์.

โฆษณายังไม่ถือว่าเพียงพอตามข้อกำหนดทางกฎหมายเพราะไม่ใช่ผู้บริโภคทุกรายที่จะมีอินเตอร์เน็ต (Internet) ยิ่งไปกว่านั้น ถ้าผู้บริโภคไม่มีโอกาสที่จะได้อ่านข้อกำหนดในสัญญาก่อนที่จะตัดสินใจทำสัญญา ข้อกำหนดในสัญญาดังกล่าวย่อมที่จะไม่มีผลผูกพัน[38]

ในประเทศนอรเวย์ คู่มือของกลุ่มพิทักษ์สิทธิผู้บริโภคว่าด้วยบริการเนื้อหาทางโทรศัพท์เคลื่อนที่ (Consumer Ombudsman's Guidelines on Mobile Content Services: CO guidelines)[39] กำหนดว่าการเปิดเผยข้อมูลอย่างน้อยจะต้องประกอบไปด้วย ราคา ชื่อผู้จัดจำหน่าย การบอกเลิกสัญญา (on-off service) ข้อจำกัดในเรื่องอายุต่างๆ รายละเอียดของสัญญา และหมายเลขโทรศัพท์ศูนย์บริการลูกค้า (customer service) ของผู้จัดจำหน่าย สำหรับการชำระค่าบริการสมาชิกนั้นก็ควรจะต้องมีข้อมูล เช่น ระยะเวลาของการชำระค่าบริการและ/หรือความถี่ในการชำระค่าบริการ สิทธิในการใช้บริการเนื้อหา (Content) ต่างๆ และหมายเลขของข้อความที่คาดหมายว่าควรจะต้องจัดให้มีด้วย

ในประเทศเกาหลี การเปิดเผยข้อมูลในกรณีข้อจำกัดของขนาดหน้าจอไม่ใช่ปัญหาที่สำคัญ แต่คณะกรรมการคุ้มครองผู้บริโภคของประเทศเกาหลี (Korean Consumer Protection Board) ได้มีการเสนอต่อรัฐบาลให้มีการพัฒนา เช่น การแจ้งข้อมูลข่าวสารทางไปรษณีย์อิเล็กทรอนิกส์ (E-mail) และการยืนยันอีกครั้งโดยผู้บริโภค

<u>การกำกับดูแลตนเองหรือการร่วมกันกำกับดูแล</u>

ในประเทศสหรัฐอเมริกา สมาคมการตลาดผ่านโทรศัพท์เคลื่อนที่ (Mobile Marketing Association: MMA) ได้มีคู่มือผู้บริโภคว่าด้วยแนวปฏิบัติอันเป็นเลิศสำหรับบริการส่งข้อมูลทางโทรศัพท์เคลื่อนที่ (Consumer Best Practices Guidelines for Cross-Carrier Mobile Content Services) กับการคำนึงถึงโปรแกรมพิเศษ (promotion programs) ซึ่งคู่มือระบุว่าผู้ให้บริการเนื้อหา (Content) ควรจะสร้างความมั่นใจ ยกตัวอย่างเช่น ข้อมูลค่าใช้บริการต้องระบุไว้อย่างชัดเจน และแสดงไว้อย่างเด่นชัด และ"ช่วย"ให้ข้อความแสดงข้อมูลในการปฏิเสธไม่รับบริการ (opt-out) ไว้อย่างชัดเจน ในประเทศแคนาดากฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์ (E-

---

[38] ยึดตามหลักในคู่มือของกลุ่มพิทักษ์สิทธิผู้บริโภคฟินแลนด์ (The guidelines of the Finnish consumer ombudsman) ตาม <www.kuluttajavirasto.fi/user_nf/default.asp?site=36&tmf=9770&lmf=9781&id=17326&mode=readdoc>.

[39] ตาม <www.forbrukerombudet.no/asset/1656/1/1656_1.pdf>.

Commerce Code) ได้สร้างกฎระเบียบพื้นฐานในส่วนของการเปิดเผยข้อมูล[40] และบทสรุปแนวปฏิบัติ (Short Code Code of Conduct) ได้กำหนดให้สมาชิกต่างๆต้องจัดให้มีข้อมูล เช่น ลักษณะเฉพาะ ข้อมูลในการปฏิเสธไม่รับบริการ (opt-out) ราคา โดยมีหน้าที่“ช่วย” และ“ให้ข้อมูล” ภายในวันและเวลาที่ข้อมูลถูกแสดง

ดังนั้น ในประเด็นการเปิดเผยข้อมูลในกรณีหน้าจอขนาดเล็ก ต้องกำหนดให้ผู้ประกอบธุรกิจจัดให้มีข้อมูลเกี่ยวกับการทำธุรกรรมทางการค้าที่ชัดเจน เหมาะสมเพื่อให้เข้าใจได้ง่าย และเป็นข้อมูลที่ถูกต้อง สามารถตรวจสอบได้ เพื่อไม่ให้เกิดความเข้าใจผิด หรือเกิดการใช้ที่ผิดพลาด และหากผู้ใช้บริการมิได้อ่านข้อสัญญาก่อนที่จะเข้าทำสัญญา ข้อกำหนดในสัญญาดังกล่าวย่อมที่จะไม่มีผลผูกพัน และอย่างน้อยข้อมูลหรือการทำสัญญานั้นต้องมีข้อมูลค่าใช้บริการที่ชัดเจนและแสดงไว้อย่างเด่นชัด ข้อความแสดงข้อมูลในการปฏิเสธไม่รับบริการ (opt-out) ข้อจำกัดในเรื่องอายุต่างๆ รายละเอียดของสัญญา และหมายเลขโทรศัพท์ศูนย์บริการลูกค้า (customer service) ของผู้จัดจำหน่าย สำหรับการชำระค่าบริการสมาชิกนั้นก็ควรจะต้องมีข้อมูล เช่น ระยะเวลาของการชำระค่าบริการและ/หรือความถี่ในการชำระค่าบริการ สิทธิในการใช้บริการเนื้อหา (Content) ต่างๆ และหมายเลขของข้อความที่คาดหมายว่าควรจะต้องจัดให้มีไว้อย่างชัดเจนด้วย นอกจากนี้ ควรให้มีการแจ้งข้อมูลโดยทางไปรษณีย์อิเล็กทรอนิกส์ (E-mail) และให้ผู้บริโภคทำการยืนยันอีกครั้งหนึ่งด้วย

2.3 แผนการคุ้มครองกรณีการใช้โทรศัพท์เคลื่อนที่โดยไม่ได้รับอนุญาต

2.3.1 การคุ้มครองภายใต้ข้อกำหนดต่าง ๆของสัญญา

เมื่อโทรศัพท์เคลื่อนที่หายหรือถูกขโมยไป และถูกนำไปใช้โดยบุคคลที่ไม่มีอำนาจ (unauthorized person) ความรับผิดในกรณีการใช้โดยไม่ได้รับความยินยอม (unauthorized use) ย่อมเป็นไปตามหลักเกณฑ์ที่กำหนดไว้ในสัญญาระหว่างผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่กับผู้บริโภคในประเทศต่างๆ รวมทั้งสาธารณรัฐเช็ก แมกซิโก นอรเวย์ สาธารณรัฐสโลวัก โปแลนด์ และสวิสเซอร์แลนด์ ยกตัวอย่างเช่น ในประเทศโปแลนด์และสาธารณรัฐสโลวัก ไม่มีกฎหมายที่คุ้มครองป้องกันในกรณีของการใช้โดยไม่ได้รับความยินยอม (unauthorized use) หรือกรณีความรับผิดสำหรับการเรียกเก็บเงินจากการใช้โดยไม่ได้รับความ

---

[40] ตัวอย่างเช่น หลักข้อที่ 1.1 กล่าวว่า ผู้ขายควรให้ข้อมูลที่เพียงพอแก่ผู้บริโภคในการเลือกว่าจะทำธุรกรรมหรือไม่ และจะทำอย่างไร

ยินยอม แต่เมื่อผู้บริโภคได้แจ้งว่าโทรศัพท์เคลื่อนที่หายหรือถูกขโมยไป บริษัทโทรศัพท์เคลื่อนที่สามารถบล็อกซิมการ์ด (SIM card) และหมายเลขหรือรหัสประจำเครื่องโทรศัพท์เคลื่อนที่ (International Mobile Equipment Identity: IMEI)[41] ได้ นอกจากนี้ รหัสบุคคล (PIN code) และการบล็อกสายเรียกเข้าและการโทรออก ก็อาจช่วยป้องกันการใช้โดยไม่ได้รับความยินยอมได้ ส่วนในประเทศนอรเวย์นั้น ถ้ามีการแจ้งต่อผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ว่าโทรศัพท์เคลื่อนที่ถูกขโมยไป ผู้บริโภคก็ไม่ต้องรับผิดชอบใดๆต่อค่าใช้จ่ายต่างๆที่ถูกเรียกเก็บในภายหลังจากที่ได้แจ้งไว้ ซึ่งการกำหนดความรับผิดก็เป็นไปตามที่กำหนดไว้ในสัญญา

2.3.2 การคุ้มครองทางโทรคมนาคม

ในประเทศฟินแลนด์ พระราชบัญญัติว่าด้วยตลาดการสื่อสาร (Communications Market Act) มาตรา 76 ได้กำหนดให้ผู้ประกอบกิจการโทรคมนาคมปิดการเชื่อมต่อสัญญาณโทรศัพท์และป้องกันการใช้โทรศัพท์ ถ้าผู้ใช้หรือหน่วยงานอื่นที่เกี่ยวข้องรายงานมาว่าโทรศัพท์เคลื่อนที่หรือสมาร์ทการ์ด (Smartcard) ที่ใช้ในโทรศัพท์เคลื่อนที่ดังกล่าวสูญหายไป และมีการร้องขอให้ปิดบริการหรือป้องกันการใช้โทรศัพท์เคลื่อนที่ ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ในฟินแลนด์บางรายก็ได้มีการเริ่มดำเนินการกำกับดูแลตนเองโดยจำกัดวงเงินค่าใช้บริการ นอกจากนั้น ในปัจจุบันกระทรวงคมนาคม (Ministry of Transport and Communication) ได้ยอมรับข้อเสนอในการขอแก้ไขพระราชบัญญัตินี้ ซึ่งจะมีผลบังคับใช้ในเดือนมีนาคม พ.ศ.2550 หนึ่งในการแก้ไขนั้นคือ จะอนุญาตให้ผู้ประกอบกิจการโทรคมนาคม และผู้บริโภคยินยอมในสัญญาที่จะจำกัดขอบเขตการใช้งาน เพื่อป้องกันการเพิ่มขึ้นอย่างไม่สามารถควบคุมได้ของจำนวนใบแจ้งราคาสินค้า เช่น การใช้งานในต่างประเทศ และการใช้บริการใหม่ต่างๆซึ่งยากแก่การคำนวณค่าใช้จ่าย[42] และผู้บริโภคยังคงต้องมีความรับผิดจากการใช้ที่ปราศจาก

---

[41] IMEI คือเลขเฉพาะ 15 หลัก ที่กำหนดในโทรศัพท์เคลื่อนที่ทุกเครื่อง ประกอบด้วย เลข 6 หลัก สำหรับรหัสการพิสูจน์ (type approval code: TAC) เลข 2 หลัก สำหรับรหัสการประกอบขั้นสุดท้าย (final assembly code: FAC) เลข 6 หลัก สำหรับรหัสประจำเครื่อง (Serial Number: SNR) และตัวเลขสำรอง (spare digit) อีก 1 หลัก

[42] องค์กรควบคุมการสื่อสารของฟินแลนด์ (Finnish Communications Regulatory Authority) ได้แยกกลุ่มเฉพาะในการป้องกันการใช้เครือข่ายไร้สายสาธารณะ (public mobile networks) และบริการข้อความสั้น (SMS) การให้บริการผ่านหมายเลขโทรศัพท์ถูกแยกตามเนื้อหาได้เป็น 1) การให้บริการทั่วไป (general services) 2) การให้คำปรึกษา (consulting) และสั่งซื้อ

ความยินยอมอยู่ หากเกิดจากความสะเพร่าของพวกเขาเอง อย่างในกรณีของการใช้บัตรเครดิตโดยไม่มีอำนาจ ในประเทศสวีเดน ข้อเสนอที่กำหนดให้ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ทุกรายจะต้องเสนอทางเลือกแก่ลูกค้าของพวกเขาที่จะทำการบล็อก (block) หมายเลขโทรศัพท์บางหมายเลขหรือสายเรียกเข้าบางสาย และกำหนดเพดานค่าบริการที่ถูกเรียกเก็บเงินของพวกเขานั้นอยู่ภายใต้การพิจารณาของรัฐบาล

2.3.3 **การคุ้มครองการชำระเงินของผู้ถือบัตร**[43]

ประเทศแคนาดา สวีเดน และสหรัฐอเมริกา ได้มีรายงานว่าการคุ้มครองบัตรชำระเงินนั้น อาจครอบคลุมไปถึงบางกรณีของการใช้โดยปราศจากความยินยอม ในประเทศเดนมาร์กนั้นเป็นกรณีพิเศษเพราะซิมการ์ด (SIM card) ในโทรศัพท์เคลื่อนที่มีลักษณะการชำระเงินอย่างเดียวกันกับบัตรชำระเงินอื่นๆซึ่งอยู่ภายใต้พระราชบัญญัติว่าด้วยเครื่องมือในการชำระเงิน (Act on Certain Payment Instrument) ตามข้อกำหนดของพระราชบัญญัติดังกล่าวกำหนดให้ผู้ออกบัตรต้องรับผิดชดใช้ต่อผู้ถือบัตรสำหรับการสูญเสียทุกกรณีที่เกิดขึ้นเนื่องจากการใช้ซิมการ์ด (SIM card) ในโทรศัพท์เคลื่อนที่โดยไม่ได้รับความยินยอม[44]

กรณีที่น่าสนใจอีกกรณีหนึ่งเกิดในประเทศอังกฤษได้มีการรณรงค์ (Immobilize campaign) ให้มีการแจ้งเพื่อระงับการบริการซึ่งจะทำให้โทรศัพท์ที่ถูกขโมยไปไม่สามารถใช้การได้และสนับสนุนให้ผู้บริโภคแจ้งถึงการขโมยนั้น[45] ซึ่งข้อมูลที่ได้รายงานไว้นั้นแม้ว่าจะมีวัตถุประสงค์

สินค้า (ordering) 3) ความบันเทิง (entertainment) และ 4) ความบันเทิงสำหรับผู้ใหญ่ (adult entertainment) ซึ่งผู้บริโภคสามารถเลือกที่จะปฏิเสธ (block) สายเข้าหรือข้อความได้ตามความต้องการ

[43] และตาม OECD (2001) และ OECD (2005a) โดยเฉพาะ p. 10-15.

[44] พระราชบัญญัติดังกล่าวได้อธิบายกรณียกเว้น 5 กรณี โดยหนึ่งกรณีในนั้นคือการใช้รหัสลับ โดยผู้ใช้ต้องเสียค่าใช้จ่ายไม่เกิน 8,000 โครนเดนมาร์ก (ประมาณ 1,280 ดอลลาร์สหรัฐ และ 1,070 ยูโร)

[45] การรณรงค์ (campaign) ได้เริ่มขึ้นในเดือนมกราคม พ.ศ.2548 และได้รับการสนับสนุนจากอุตสาหกรรมโทรศัพท์เคลื่อนที่ (Mobile phone industry) ผ่านการกลุ่มปฏิบัติการต่อต้านอาชญากรรมอุตสาหกรรมเคลื่อนที่ (Mobile Industry Crime Action Forum) หน่วยอาชญากรรมโทรศัพท์เคลื่อนที่แห่งชาติ (National Mobile Phone Crime Unit) ในหน่วยบริการตำรวจแห่งชาติ (Metropolitan Police Service) และหน่วยตำรวจสหราชอาณาจักร (UK police

หลักเพื่อช่วยลดอัตราของอาชญากรรมบนท้องถนนก็ตาม แต่การรายงานดังกล่าวก็ยังสามารถช่วยให้ความรับผิดในค่าเสียหายต่างๆจากการใช้โดยไม่ได้รับความยินยอมของผู้บริโภคสิ้นสุดลงอีกด้วย

ดังนั้น ในประเด็นการใช้โดยไม่ได้รับอนุญาต เมื่อโทรศัพท์เคลื่อนที่หายหรือถูกขโมยไป ต้องกำหนดให้ผู้ใช้บริการแจ้งถึงการหายหรือถูกขโมยไป เพื่อให้บริษัทโทรศัพท์เคลื่อนที่สามารถระงับบริการหรือสัญญาณ หรือบล็อกซิมการ์ด (SIM card) และหมายเลขหรือรหัสประจำเครื่องโทรศัพท์เคลื่อนที่ (IMEI) ได้ และเพื่อที่ผู้ใช้บริการจะไม่ต้องรับผิดชอบต่อค่าใช้จ่ายที่เกิดขึ้นภายหลังจากที่ได้แจ้งไว้ แต่ทั้งนี้ ผู้บริการยังคงต้องมีความรับผิดจากการใช้ที่ปราศจากความยินยอมอยู่ หากเกิดจากความสะเพร่าของตนเอง และต้องกำหนดให้ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ทุกราย เสนอทางเลือกแก่ผู้ใช้บริการที่จะทำการบล็อก (block) สายเรียกเข้าและการโทรออก จำกัดขอบเขตการใช้งาน และกำหนดเพดานค่าบริการที่ถูกเรียกเก็บเงินในบริการบางอย่างเช่น การใช้งานในต่างประเทศ หรือบริการที่ยากแก่การคำนวณค่าใช้จ่าย นอกจากนี้ การตั้งรหัสบุคคล (PIN code) ก็อาจช่วยป้องกันการใช้โดยไม่ได้รับความยินยอมได้

---

force) อื่นๆอีก 38 หน่วย ในปี พ.ศ. 2548 Immobilize ได้รับข้อมูลของโทรศัพท์ประมาณ 10 ล้านเครื่อง ซึ่งเจ้าของโทรศัพท์ได้ลงทะเบียนเลข IMEI ของตัวเองไว้แล้ว คำแนะนำในการป้องกันอาชญากรรมเกี่ยวกับโทรศัพท์เคลื่อนที่ปรากฏในเว็บไซต์ของ Immobilize, ที่ <https://www.immobilise.com/home.ikml>.

2.4 SMS spam[46]

พระราชบัญญัติหรือกฎหมายต่างๆว่าด้วยการต่อต้านข้อมูลที่ไม่พึงประสงค์ (Anti-Spam Act or provisions) ส่วนใหญ่ ครอบคลุมถึงข้อมูลที่ไม่พึงประสงค์ผ่านทางข้อความสั้น (SMS) เช่น Australia's Spam Act 2003, Belgium's Act of 11 March 2003 on electronic commerce, Czech Republic's Act on Some Services of the Information Society, Slovak Republic's Act on Advertising and on Electronic Communication, Norway's Market Control Act มาตรา 2b, United States' Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) และ European Union's Directive 2002/58/EC โดยหากผู้ใช้โทรศัพท์เคลื่อนที่ไม่ยอมที่จะรับฐานข้อมูลการโฆษณา (information-based advertisements) ต่างๆ เช่นนี้แล้ว การโฆษณานั้นก็จะถูกพิจารณาว่าเป็นข้อมูลที่ไม่พึงประสงค์ (Spam)[47]

แม้ในต่างประเทศจะถือว่าการส่ง Spam SMS เป็นเสรีภาพในการโฆษณาของเจ้าของสินค้า แต่หลายความเห็นก็ถือว่า Spam SMS นั้นได้ละเมิดสิทธิส่วนบุคคลของผู้รับ Spam SMS เนื่องจากเป็นการส่งเมล์ที่ผู้รับไม่ต้องการและไม่ได้ร้องขอ ดังนั้น ในประเทศสหรัฐอเมริกาจึง

---

[46] คณะทำงานพิเศษเกี่ยวกับข้อมูลที่ไม่พึงประสงค์ (Special Spam Task Force) ขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development: OECD) ได้พิจารณาในประเด็นข้อมูลที่ไม่พึงประสงค์ในรูปของข้อความสั้น (SMS spam) และได้แถลงการณ์ในเรื่องข้อเสนอแนะของคณะกรรมการในเรื่องของการบังคับใช้ระหว่างประเทศ (cross-border enforcement) ในการร่วมมือกับคณะกรรมาธิการว่าด้วยนโยบายด้านข้อมูลข่าวสาร คอมพิวเตอร์ และการติดต่อสื่อสาร (Committee for Information, Computer and Communications Policy: ICCP) และคณะกรรมาธิการว่าด้วยนโยบายด้านผู้บริโภค (Committee on Consumer Policy: CCP) ตาม DSTI/CP/ICCP/SPAM(2005)3/FINAL.

[47] กลุ่มผู้บริโภคเช่น กลุ่มเจรจาผู้บริโภคสองฟากฝั่งมหาสมุทรแอตแลนติก (Trans Atlantic Consumer Dialogue: TACD) ได้มุ่งเน้นให้มีการออกข้อบังคับอย่างชัดเจน มิเช่นนั้นผู้บริโภคจะเสี่ยงกับการได้รับข้อเสนอที่ไม่พึงประสงค์ (unsolicited offers) ทางโทรศัพท์เคลื่อนที่มากเกินความจำเป็น นอกจากนี้ กลุ่มเจรจาผู้บริโภคสองฟากฝั่งมหาสมุทรแอตแลนติกยังได้เสนอแนะให้ป้องกันการโฆษณาที่ไม่พึงประสงค์ (unsolicited advertisements) สำหรับสินค้าหรือบริการทุกอย่างที่ถูกส่งไปยังโทรศัพท์เคลื่อนที่ของผู้บริโภค (TACD, 2005).

ได้มีการออกกฎหมาย CAN-SPAM Act of 2003 ออกมาควบคุม Spam Mail ซึ่งมีข้อกำหนดต่างๆ ที่ครอบคลุมถึงข้อมูลที่ไม่พึงประสงค์ผ่านทางข้อความสั้น (SMS) เช่น ผู้ส่ง Spam Mail จะต้องมีขั้นตอนการยกเลิกการรับ Spam Mail นั้น ผู้ส่งจะต้องแสดงในหัวข้อข้อความสั้น (SMS) ว่าเป็นข้อความสั้น (SMS) เพื่อการโฆษณา แสดงที่อยู่หรือที่อยู่ทางไปรษณีย์อิเล็กทรอนิกส์ (email address) จริงที่ผู้รับสามารถติดต่อกลับได้ และห้ามปลอมแปลงแหล่งที่มาของข้อความสั้น (SMS) และ Spam Mail นั้นจะต้องไม่ละเมิดผู้รับ ไม่ว่าจะเป็นการใช้โปรแกรมที่แฝงมาในไปรษณีย์อิเล็กทรอนิกส์ (E-mail) หรือข้อความสั้น (SMS) เพื่อขโมยเอาข้อมูลในเครื่องของผู้รับ การส่งไวรัสหรือการใช้ Trojan Horse หรือ worms และ CAN-SPAM Act of 2003 มีข้อกำหนดในเรื่อง “opt-out instructions” โดยความคิดที่ว่าผู้รับน่าจะมีสิทธิในการเลือกที่จะรับหรือไม่รับข้อความสั้น (SMS) ได้ ซึ่งถือเป็นวิธีที่น่าสนใจในการสร้างสมดุลระหว่างเสรีภาพในการโฆษณาของผู้ส่ง และสิทธิส่วนบุคคลในการเลือกที่จะรับหรือไม่รับข้อความสั้น (SMS) ของผู้รับ

นอกจากนี้ ตาม DSTI/CP/ICCP/SPAM(2005)10/FINAL ได้มีการกำหนดในเรื่องการให้ความยินยอม (consent) ว่า หลักการพื้นฐานที่เกี่ยวข้องกับการจัดการควบคุมต่อต้านข้อมูลขยะต่างๆ (anti-spam regulatory arrangements) คือ การส่งไปรษณีย์อิเล็กทรอนิกส์ (e-mail)[48] เพื่อการค้าสามารถทำได้เพียงส่งไปยังเอกชน (individuals) หรือองค์กร (organizations) ที่ได้ให้ความยินยอมในการรับสิ่งเหล่านั้น จำนวนของกรอบความคิดเป็นประโยชน์ต่อความเกี่ยวพันกับความยินยอม รวมถึงแบบและกฎหมายในการอนุญาตและการปฏิเสธ (opt-in and opt-out models and provisions) ซึ่งยอมรับการให้ความยินยอมซึ่งอนุมานได้จากความสัมพันธ์ที่มีก่อนหน้านั้น (pre-existing relationship)

หนึ่งในปัญหาพื้นฐานที่สุดเกี่ยวกับออกกฎหมายหรือการวางข้อกำหนดข้อมูลขยะ (spam legislation or regulation) เชื่อมโยงกับปัญหาการให้ความยินยอม (consent) หรือบางครั้งมีรูปแบบเป็นการอนุญาต (opt-in) หรือการปฏิเสธ (opt-out) หรือทั้งสองอย่าง การกระทำนั้นอยู่บนพื้นฐานความยินยอมของผู้รับ (ข้อกำหนดการค้าบนพื้นฐานความยินยอม (permission-based marketing)) ก่อนได้รับข้อความอิเล็กทรอนิกส์ (electronic message) ในการอนุญาต

---

[48] ซึ่งตาม DSTI/CP/ICCP/SPAM(2005)10/FINAL หน้า 5 นั้นรวมถึงข้อความสำเร็จรูป (Instant Messaging) ข้อความสั้น (Short Message Service: SMS) ข้อมูลขยะทางโทรศัพท์และข้อความทางโทรศัพท์รูปแบบอื่น (Other mobile spam and mobile messaging formats) อย่างการส่งข้อความมัลติมีเดีย (multimedia messaging service: MMS) โทรสาร (Facsimile).

หรือภายหลังได้รับข้อความอิเล็กทรอนิกส์ในการปฏิเสธ เช่นเดียวกันกับการระบุชื่อที่ชัดเจนและการออกกฎหมาย แนวคิดในเรื่องความยินยอมก็สามารถรวมเข้ากับการใช้ระบบความเป็นส่วนตัวของบุคคลและข้อมูล ซึ่งอาจรวมกับข้อสันนิษฐานว่าหากปราศจากการให้ความยินยอม บุคคลไม่อาจเข้าสู่ ขาย หรือแลกเปลี่ยนข้อมูลที่เฉพาะเจาะจง อย่างเช่น ที่อยู่ทางไปรษณีย์อิเล็กทรอนิกส์ (e-mail address) ปัญหาที่สำคัญคือ ระดับของความยินยอมหรือการอนุญาตซึ่งผู้ออกกฎหมายหรือผู้ควบคุมมุ่งหวังที่จะบังคับใช้ในกรณีที่เฉพาะเจาะจง

<u>โทษที่บังคับใช้ในข้อความที่ไม่พึงประสงค์ (SMS Spam)</u>

ในส่วนโทษปรับที่บังคับใช้ในข้อความที่ไม่พึงประสงค์ (SMS Spam)[49] ผู้ให้บริการโทรคมนาคม (telecommunications provider) ถูกปรับเป็นเงิน 110,000 เหรียญสหรัฐหลังจากที่ส่งข้อความสั้น (SMS messages) โดยปราศจากการแสดงตัวผู้ส่งที่เพียงพอ (sender identification) ซึ่งโทษปรับได้ถูกนำมาบังคับใช้โดยคณะกรรมการกิจการโทรคมนาคมและสื่อมวลชนแห่งชาติประเทศออสเตรเลีย (Australian Communication and Media Authority: ACMA) สำหรับการฝ่าฝืน Spam Act 2003

Spam Act 2003 ได้นำมาปรับใช้กับข้อความพาณิชย์อิเล็กทรอนิกส์ (commercial electronic messages) ทั้งไปรษณีย์อิเล็กทรอนิกส์ (email) ข้อความสั้น (SMS) ข้อความมัลติมีเดีย (MMS) และข้อความสำเร็จรูป (instant messaging) Spam Act 2003 ได้กำหนดให้ข้อความพาณิชย์อิเล็กทรอนิกส์ (commercial electronic messages) รวมถึง "ข้อมูลของผู้ส่งที่ถูกต้อง" (accurate sender information) ในกรณีนี้บริษัทผู้ให้บริการมิได้ระบุชื่อของตนเองหรือชื่อของสินค้า ในการโต้แย้งดังกล่าวผู้รับสามารถสร้างการเชื่อมต่อระหว่าง three-digit sender ID และ three-letter product name ซึ่งคณะกรรมการกิจการโทรคมนาคมและสื่อมวลชนแห่งชาติประเทศออสเตรเลีย (Australian Communication and Media Authority: ACMA) ไม่อาจยอมรับการโต้แย้งดังกล่าวได้ ในขณะที่นักการตลาดทางข้อความสั้น (SMS marketers) พยายามที่จะแสดงข้อความทั้งหมดของพวกเขาลงในพื้นที่ขนาดเล็กที่จำกัดจำนวนตัวอักษรของข้อความ (small per-message character limits) คณะกรรมการกิจการโทรคมนาคมและสื่อมวลชน

---

[49] ดูข้อมูลเพิ่มเติมได้ที่ <http://www.uslaw.com/library/Intellectual_Property_Law/Fines_Imposed_SMS_Spam.php?item=352749>.

แห่งชาติประเทศออสเตรเลีย (Australian Communication and Media Authority: ACMA) ก็ได้แสดงให้เห็นในส่วนนี้ว่าถูกจำกัดให้ยอมรับต่อการย่นย่อ

คณะกรรมการกิจการโทรคมนาคมและสื่อมวลชนแห่งชาติประเทศออสเตรเลีย (Australian Communication and Media Authority: ACMA) ก็ไม่สามารถที่จะบรรลุข้อตกลงกับบริษัทผู้ให้บริการในข้อกำหนดที่บังคับให้ปฏิบัติตามสัญญา (an enforceable undertaking) ในประเด็นค่าปรับ คณะกรรมการกิจการโทรคมนาคมและสื่อมวลชนแห่งชาติประเทศออสเตรเลีย (Australian Communication and Media Authority: ACMA) ได้กล่าวว่าจะนำการบังคับใช้ที่มีอำนาจเข้มแข็งกว่ามาใช้กับข้อเสนอที่ผูกพัน (undertakings offered) ไม่ได้พิจารณาประเด็นการยอมปฏิบัติที่เพียงพอที่เพิ่มขึ้น

คณะกรรมการกิจการโทรคมนาคมและสื่อมวลชนแห่งชาติประเทศออสเตรเลีย (Australian Communication and Media Authority: ACMA) ได้มีการเปิดเผยว่า 55% ของการร้องเรียนของผู้ลงทะเบียนไม่รับสาย (Do Not Call Register complaints) ได้รับในข่ายกิจการโทรคมนาคม (telecommunications sphere) ซึ่งเป็นผลมาจากแผนการส่งเสริมทางโทรศัพท์ของสายที่ไม่ต้องการและบริการที่เกี่ยวข้อง

ข้อห้ามหรือระวางโทษของข้อมูลขยะ[50] การนำกฎหมายต่อต้านข้อมูลขยะ (anti-spam legislation) และวิธีการควบคุม (regulatory measures) มาบังคับใช้ไม่อาจพิจารณาอย่างวิธีการแก้ปัญหาในปัญหาข้อมูลขยะ (spam) เนื่องจากไม่มี silver bullet ที่จะหยุดการส่งข้อความดังกล่าว โดยเฉพาะอย่างยิ่ง เนื่องจากค่าใช้จ่ายในการส่งข้อความดังกล่าวต่ำ ลำพังการออกกฎหมายเพียงอย่างเดียวไม่สามารถที่จะหยุดยั้งการส่งข้อมูลขยะที่อาจเกิดขึ้นได้ (potential spammers) จากการตักตวงผลประโยชน์ในตลาดเทคโนโลยี (marketing technique) นี้ การส่งข้อมูลขยะซึ่งผิดกฎหมาย (illegitimate spam) ถือเป็นการละเลยข้อกำหนดของกฎหมาย (legislative provisions) อย่างแท้จริง อย่างไรก็ตาม กฎหมายที่ควบคุมข้อมูลขยะ (spam) สามารถให้วัตถุประสงค์อันเป็นแนวคิดเบื้องต้นเกี่ยวกับนโยบายสาธารณะที่มีประโยชน์ในการลงโทษเหล่าเอกชน (individuals) และองค์กร (organizations) ที่เลือกใช้วิธีการนี้สร้างความเสียหายให้แก่ผู้บริโภค และดังนั้นพระราชบัญญัติจึงเป็นเสมือนสิ่งที่ขัดขวางเหล่าเอกชน (individuals) และองค์กร (organizations) ที่คิดจะใช้ไปในทางนี้ ภายในกรอบที่สร้างความชัดเจน

---

[50] ตาม DSTI/CP/ICCP/SPAM(2005)10/FINAL, ดูข้อมูลเพิ่มเติมได้ที่ <http://www.oecd.org/dataoecd/29/12/35670414.pdf>.

ซึ่งเป็นเครื่องมือสำคัญในการห้ามปรามพฤติกรรมเช่นว่านั้น การกระทำดังกล่าวถือเป็นการฝ่าฝืนกฎหมายและก่อให้เกิดผลร้ายแรงจากการละเมิดของพวกเขา

<u>การกำกับดูแลตนเองของผู้ประกอบธุรกิจโทรคมนาคม (Telecommunication operators)</u>

เป็นวิธีการที่มีประสิทธิภาพในการต่อต้านข้อมูลที่ไม่พึงประสงค์ (Spam) ผ่านอุปกรณ์โทรศัพท์เคลื่อนที่ โดยทั่วไปผู้ประกอบธุรกิจ (operators) ใช้ระบบการคัดกรองเพื่อปฏิเสธการรับข้อความสั้น (SMS) ที่มี URLs และหมายเลขโทรศัพท์อยู่ในข้อความ ท่ามกลางมาตรการอื่นๆ ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ (mobile carriers) ในประเทศญี่ปุ่น ได้จำกัดจำนวนไปรษณีย์อิเล็กทรอนิกส์ (E-mail) ที่ส่ง และสายที่ต้องสงสัยว่าเป็นข้อมูลที่ไม่พึงประสงค์ (suspend lines of spammers) ที่ส่งมาทางข้อความสั้น (SMS) และไปรษณีย์อิเล็กทรอนิกส์ทางอินเตอร์เน็ต (internet e-mail) มายังโทรศัพท์เคลื่อนที่[51] ในประเทศสวิสเซอร์แลนด์ ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ (mobile carriers) ได้คิด “ค่าธรรมเนียมการสื่อสารระหว่างเครือข่าย” (interworking fees) โดยคิดจากข้อความสั้น (SMS) ที่เข้ามาสู่เครือข่ายของพวกเขาเพื่อที่จะจำกัดการเข้ามาของการขายที่ไม่พึงประสงค์ทางโทรศัพท์เคลื่อนที่ (mobile spam)

ความพยายามของภาคอุตสาหกรรมระหว่างประเทศก็มีความสำคัญต่อการต่อสู้กับข้อมูลที่ไม่พึงประสงค์ทางข้อความสั้น (SMS spam) เพราะข้อมูลที่ไม่พึงประสงค์ทางโทรศัพท์เคลื่อนที่ (mobile spam) นั้นส่งข้ามเครือข่าย หรือระหว่างประเทศ ซึ่งสมาคมจีเอสเอ็ม (GSM Association: GSMA) ได้มีการพัฒนาข้อมูลและสนับสนุนกระบวนการที่จะช่วยให้ผู้ประกอบธุรกิจโทรศัพท์เคลื่อนที่ (mobile operators) ทำงานร่วมกันเพื่อระบุและจัดการกับปัญหานี้ และได้มีการตั้งคณะทำงานระหว่างประเทศในเรื่องการขายที่ไม่พึงประสงค์ทางโทรศัพท์เคลื่อนที่ (International working groups on mobile spam) จากสิ่งที่กล่าวมาทำให้เกิดความร่วมมือระหว่างประเทศ และเกิดการแลกเปลี่ยนแนวปฏิบัติที่ดีที่สุด (best practices) ในระหว่างผู้ให้บริการ สมาคมจีเอสเอ็ม (GSM Association: GSMA) ยังได้พัฒนาแนวปฏิบัติที่มิใช่ทางด้านกฎหมาย โดยความร่วมมือของผู้ให้บริการโทรศัพท์เคลื่อนที่ 15 ราย ที่ได้ลงนามร่วมกันใน

---

[51] องค์กรควบคุมการสื่อสารของฟินแลนด์ (Finnish Communications Regulatory Authority) ได้กล่าวด้วยว่า ผู้ให้บริการต้องปกป้องการถ่ายโอนข้อมูลและการรับข้อความ กำจัดซอฟท์แวร์ที่เป็นอันตรายต่อความปลอดภัยของข้อมูลจากข้อความเหล่านั้น และใช้วิธีทางเทคนิคเข้าช่วย เพื่อรักษาความปลอดภัยของข้อมูลในการบริการ

เดือนกุมภาพันธ์ พ.ศ. 2549 นอกจากนี้ ในเดือนกันยายน พ.ศ. 2549 สภาหอการค้าระหว่างประเทศ (ICC) ได้จัดทำข้อปฏิบัติว่าด้วยการโฆษณาและการสื่อสารการตลาด (A Code of Advertising and Marketing Communication Practice) ซึ่งกล่าวถึงการซื้อขายสินค้าหรือบริการที่มิได้ร้องขอผ่านทางโทรศัพท์เคลื่อนที่จะถูกส่งเฉพาะเมื่อมีหลักฐานอันสมควรให้เชื่อว่าผู้บริโภคจะให้ความสนใจในเรื่องหรือข้อเสนอดังกล่าว (ข้อ D5)[52]

ดังนั้น ในประเด็นข้อความที่ไม่พึงประสงค์ (SMS Spam) หากผู้ใช้โทรศัพท์เคลื่อนที่ไม่ยอมที่จะรับฐานข้อมูลการโฆษณาต่างๆแล้ว การโฆษณานั้นก็จะถูกพิจารณาว่าเป็นข้อมูลที่ไม่พึงประสงค์ (Spam) และการส่งข้อความสั้น (SMS) เพื่อการค้าจะกระทำได้เมื่อได้รับความยินยอมจากผู้รับก่อน ซึ่งเป็นการอนุญาต (opt-in) ก่อนได้รับข้อความอิเล็กทรอนิกส์ (electronic message) และผู้ให้บริการต้องจัดให้มีขั้นตอนในการปฏิเสธ (opt-out) ภายหลังได้รับข้อความอิเล็กทรอนิกส์ (electronic message) ที่ผู้รับมีสิทธิในการเลือกที่จะรับหรือไม่รับข้อความสั้น (SMS) ได้ อีกทั้ง ผู้ส่งจะต้องแสดงในหัวข้อข้อความสั้น (SMS) ว่าเป็นข้อความสั้น (SMS) เพื่อการโฆษณา แสดงชื่อ ชื่อสินค้า ที่อยู่หรือที่อยู่ทางไปรษณีย์อิเล็กทรอนิกส์ (email address) จริงที่ผู้รับสามารถติดต่อกลับได้ และห้ามปลอมแปลงแหล่งที่มาของข้อความสั้น (SMS) และ SMS Spam นั้นจะต้องไม่ละเมิดผู้รับ ข้อมูลขยะซึ่งผิดกฎหมาย ถือเป็นการละเลยข้อกำหนดของกฎหมาย นอกจากนี้ ผู้ให้บริการอาจถูกปรับหากฝ่าฝืน Spam Act 2003 เช่น หากส่งข้อความสั้น (SMS messages) โดยปราศจากการแสดงตัวผู้ส่งที่เพียงพอ (sender identification)

2.5 การคุ้มครองผู้เยาว์

อัตราการใช้โทรศัพท์เคลื่อนที่ของผู้เยาว์มีอัตราเพิ่มสูงขึ้น โดยเฉพาะในส่วนของการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (m-commerce) มีผู้แสดงความคิดเห็นบางรายตั้งข้อสังเกตว่าปัญหาต่างๆที่เกิดขึ้นจากการใช้โทรศัพท์เคลื่อนที่ของผู้เยาว์นั้นก่อให้เกิดความล้มเหลวในความสัมพันธ์ของครอบครัวและจากผลดังกล่าวจึงต้องการการแก้ไขอย่างจริงจัง[53] ความเสี่ยง

---

[52] โปรดดูที่ <www.iccwbo.org/policy/marketing/id8532/index.html>.

[53] นาย Denis Nelthorpe ศูนย์กฎหมายคุ้มครองผู้บริโภควิคตอเรีย (Consumer Law Centre Victoria) ประเทศออสเตรเลีย ได้กล่าวไว้ในการประชุมผู้เชี่ยวชาญในเรื่องเด็กโทรศัพท์เคลื่อนที่และอินเตอร์เน็ต ในวันที่ 6-7 มีนาคม พ.ศ. 2546 ตาม IAJ (2003).

หลักๆที่ผู้เยาว์ได้รับในการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (m-commerce) นั้นมีดังจะได้กล่าวต่อไปนี้

2.5.1 **สถานภาพทางกฎหมายของผู้เยาว์ที่เข้าทำธุรกรรม**

ในหลายๆประเทศได้มีการกำหนดให้การเข้าทำธุรกรรมทางพาณิชย์ของผู้เยาว์ต้องได้รับอนุญาตจากผู้ปกครองก่อน ในกฎหมายแพ่งของประเทศญี่ปุ่นนั้นกำหนดให้ผู้เยาว์จะต้องได้รับการอนุญาตจากผู้แทนโดยชอบธรรมตามกฎหมายเมื่อจะกระทำการทางกฎหมายและหากการกระทำใดได้กระทำไปโดยปราศจากความเห็นชอบของผู้แทนโดยชอบธรรมก็อาจจะถูกเพิกถอนได้ ในประเทศฟินแลนด์ตามข้อกำหนดของ Guardianship Service Act มาตรา 23 และ 24 ได้กำหนดว่าบุคคลที่อายุต่ำกว่า 18 ปี จะถูกจำกัดความสามารถตามกฎหมายและสามารถที่จะเข้าทำได้แต่เฉพาะธุรกรรมทั่วไปที่ไม่ก่อให้เกิดผลใดๆมากนัก ผู้เยาว์ไม่มีสิทธิในการก่อหนี้ มีเพียงสิทธิเข้าทำธุรกรรมเงินสด แต่การซื้อสินค้าผ่านทางโทรศัพท์เคลื่อนที่จะถูกเรียกเก็บเงินในภายหลัง ดังนั้น เมื่อผู้ให้บริการตั้งเป้าที่เด็กโดยใช้บริการพิเศษและมีการพัฒนาบริการใหม่ๆเพื่อกลุ่มเป้าหมายที่เป็นเด็ก ผู้ปกครองไม่ควรจะต้องแบกรับความรับผิดชอบทั้งหมดสำหรับสถานการณ์ต่างๆที่จะเกิดขึ้นได้ ผู้ให้บริการจะต้องใคร่ครวญว่าผู้เยาว์ไม่เหมือนคู่สัญญาที่เป็นผู้ใหญ่ และยังได้มีการตั้งคำถามในสิทธิของผู้ให้บริการเครือข่ายโทรคมนาคมที่จะคิดค่าบริการในการทำธุรกรรมที่ไม่สมบูรณ์หรือไม่

ในบางประเทศได้มีการกำหนดห้ามมิให้ผู้เยาว์ที่มีอายุต่ำกว่าเกณฑ์ที่กำหนดเข้าทำสัญญา ถึงแม้ว่าพวกเขาจะได้รับการอนุญาตจากผู้ปกครองก็ตาม ยกตัวอย่างเช่น ในประเทศเบลเยี่ยม บุคคลที่อายุต่ำกว่า 18 ปีไม่สามารถที่จะเข้าทำสัญญาต่างๆได้ ตามกฎหมายแพ่ง มาตรา 1124 ในประเทศเยอรมัน ตามกฎหมายแพ่ง (BGB) กำหนดว่าเด็กอายุต่ำกว่า 7 ปี ไม่มีความสามารถพอที่จะทำสัญญาได้ (กฎหมายแพ่ง มาตรา 104) ในขณะที่บุคคลอายุระหว่าง 7-18 ปี อาจเข้าทำสัญญาได้ในกรณีที่ได้รับความยินยอมจากผู้ปกครอง (กฎหมายแพ่ง มาตรา 1106) ในฮังการีการเข้าทำสัญญาทุกชนิดของเด็กที่มีอายุต่ำกว่า 14 ปี จะต้องกระทำโดยผู้ปกครอง ส่วนเด็กที่มีอายุระหว่าง 14-18 ปี นั้นจะต้องได้รับความยินยอมจากผู้ปกครองก่อนหรือภายหลังการทำสัญญา ในโปแลนด์สัญญาที่ทำขึ้นโดยผู้เยาว์ที่มีอายุต่ำกว่า 13 ปี นั้นเป็นโมฆะ และสัญญาที่ทำขึ้นโดยบุคคลที่มีอายุระหว่าง 13-18 ปี นั้นจะมีผลตามกฎหมายเฉพาะเมื่อได้รับอนุญาตจากผู้ปกครอง

2.5.2 มาตรการในการจัดการกับกรณีการบริโภคมากเกินสมควรของผู้เยาว์

ในหลายๆประเทศได้มีการบังคับให้บิดามารดาหรือผู้ปกครองตามกฎหมายมีสิทธิและหน้าที่ที่จะต้องรับผิดชอบต่อการกระทำทางกฎหมายของเด็กที่อยู่ในความปกครอง เช่น ตามกฎหมายแพ่งของประเทศแมกซิโก มาตรา 1919 ตามกฎหมายแพ่งของเยอรมัน (BGB) มาตรา 1626 อนุมาตรา 1

แม้ว่าไม่มีประเทศสมาชิกใดที่มีข้อกำหนดกฎหมายที่กำหนดในส่วนของระดับการบริโภคของผู้เยาว์ก็ตาม ผู้ควบคุมดูแลในบางประเทศก็มีความตั้งใจที่จะควบคุมให้ธุรกิจการซื้อขายสินค้าหรือบริการ และข้อตกลงในสัญญาเป็นไปตามที่กฎระเบียบที่เกี่ยวข้องกำหนด ยกตัวอย่างเช่น ในประเทศนอรเวย์ ผู้ปกครองมีความรับผิดชอบต่อผู้เยาว์ แต่ในคู่มือของกลุ่มพิทักษ์สิทธิผู้บริโภคว่าด้วยบริการเนื้อหาทางโทรศัพท์เคลื่อนที่ (Consumer Ombudsman's Guidelines on Mobile Content Services: CO guidelines) ได้มีการกำหนดรายการบางอย่างให้ผู้ประกอบธุรกิจต้องปฏิบัติตามในการซื้อขายสินค้าหรือบริการและการขายบริการเนื้อหาทางโทรศัพท์เคลื่อนที่ (Mobile Content) แก่ผู้เยาว์[54] โดยกลุ่มพิทักษ์สิทธิผู้บริโภค (Ombudsman) ได้กำหนดเพดานการให้บริการในกลุ่มเป้าหมายที่เป็นผู้เยาว์ไว้ในบท (Chapters) ที่ 5.4 และ 5.5 ของคู่มือ (guidelines) ตัวอย่างเช่น กลุ่มพิทักษ์สิทธิผู้บริโภค (Consumer Ombudsman) ต้องพิจารณาการฝ่าฝืนพระราชบัญญัติว่าด้วยการควบคุมการตลาด (Marketing Control Act: MCA) ซึ่งเกิดขึ้นได้หากผู้ให้บริการเนื้อหา (Content) ไม่ได้กำหนดขอบเขตในแต่ละเดือนให้อยู่ประมาณ 1,000 นอร์วีเจียนโครน (145 เหรียญสหรัฐและ 125 ยูโร) รวมภาษี สำหรับการซื้อบริการจากหมายเลขที่เข้าใช้บริการ และสำหรับบริการข่าวสารรายเดือนสำหรับสมาชิก (subscription services) มีกำหนดเพดานอยู่ที่ 100 นอร์วีเจียนโครน กลุ่มพิทักษ์สิทธิผู้บริโภคฟินแลนด์ (Finnish Consumer Ombudsman) ยังได้ให้ความสำคัญต่อหน้าที่ของผู้ให้บริการที่จะต้องจัดให้มีบริการที่เป็นธรรมและเป็นไปตามกฎหมายเมื่อกลุ่มเป้าหมายทางธุรกิจของพวกเขาเป็นผู้เยาว์ แม้ว่าบิดามารดามีหน้าที่ตามกฎหมายอย่างผู้ปกครองแล้วก็ตาม ในเกาหลีพระราชบัญญัติว่าด้วยการคุ้มครองผู้บริโภคในการพาณิชย์อิเล็กทรอนิกส์ (Act on Consumer Protection in Electronic Commerce) ได้กำหนดให้ผู้ประกอบธุรกิจต้องแจ้งรายละเอียดต่อผู้เยาว์ว่า สัญญาสามารถทำ

[54] <www.forbrukerombudet.no/asset/1656/1/1656_1.pdf>.

การยกเลิกได้โดยผู้เยาว์หรือผู้ปกครอง ถ้าผู้ปกครองไม่ได้ให้ความเห็นชอบในการเข้าทำสัญญาดังกล่าว[55]

นอกจากนี้ ภาคอุตสาหกรรมยังได้มีการพัฒนาแนวปฏิบัติ อย่างในประเทศแคนาดามีแนวปฏิบัติที่เกี่ยวข้องคือ ข้อปฏิบัติสำหรับการคุ้มครองผู้บริโภคในการพาณิชย์อิเล็กทรอนิกส์ประเทศแคนาดา (Canadian Code of Practice for Consumer Protection in Electronic Commerce) และบทสรุปแนวปฏิบัติ (Short Code Code of Conduct) บทบัญญัติแรกได้กำหนดให้ผู้ขายต้องดำเนินการทุกขั้นตอนอย่างเหมาะสมเพื่อป้องกันผู้เยาว์ทำธุรกรรมทางการเงิน ส่วนบทบัญญัติหลังนั้น ได้กำหนดให้โปรแกรมรวบรวมข้อมูล (Aggregator) จะต้องยืนยันได้ว่าผู้ใช้แต่ละคนมีอายุตามที่กฎหมายในแต่ละท้องถิ่นกำหนด ก่อนที่จะอนุญาตให้ผู้ใช้ดังกล่าวเข้าร่วมในโปรแกรมหรือรับข้อความ ในสหราชอาณาจักร ผู้ประกอบการด้านโทรคมนาคม รวมถึงผู้ประกอบการโทรศัพท์เคลื่อนที่ ได้เห็นชอบต่อบันทึกความเข้าใจ (MoU) โดยสมัครใจเพื่อเฝ้าระวังสัญญาณ และใช้ข้อมูลร่วมกันหลังจากการพิจารณาค่าบริการโดยสำนักงานการสื่อสาร (Ofcom)

นอกจากนี้ ยังได้มีการร่วมกันในมาตรการทางเทคโนโลยี ในออสเตรเลีย โดยทั่วไปได้มีการใช้หมายเลขรหัสบุคคล (PIN) ในการควบคุมการเข้าใช้บริการเนื้อหา (Content) สำหรับผู้ใหญ่ของเด็ก อย่างเช่น บริการลามกทางโทรศัพท์ (telephone sex) มาตรการอีกอย่างนั้นรวมไปถึงการพิสูจน์อายุเพื่อให้แน่ใจว่าเด็กไม่ได้เข้าใช้บริการสำหรับผู้ใหญ่ ผู้ประกอบกิจการโทรศัพท์เคลื่อนที่ (Mobile phone operators) มีวิธีการควบคุมโทรศัพท์เคลื่อนที่ของเจ้าของที่เป็นผู้เยาว์ที่มีอายุต่ำกว่า 18 ปีที่ได้จดทะเบียนไว้ทำให้โทรศัพท์เคลื่อนที่เครื่องนั้นไม่สามารถที่จะเข้าใช้บริการสำหรับผู้ใหญ่ได้ ในประเทศญี่ปุ่น แนวทางปฏิบัติว่าด้วยการค้าอิเล็กทรอนิกส์ (E-Commerce Guidelines)[56] ชี้ให้เห็นว่าธุรกิจที่จำกัดอายุของผู้ใช้เพื่อปรับใช้กับแนวคิด ***frudulent information*** โดยผู้เยาว์ในมาตรา 20 แห่งกฎหมายแพ่ง (Civil Code) อาจจะไม่เพียงพอ

2.5.3 แผนการคุ้มครองในกรณีการเข้าถึงบริการที่ไม่เหมาะสมโดยผู้เยาว์

ในกรณีนี้มีเพียงประเทศเดียวที่มีข้อกำหนดที่ครอบคลุมถึงการให้บริการทุกประเภทแก่ผู้เยาว์ ในประเทศแคนาดา พระราชบัญญัติคุ้มครองผู้บริโภคของแคว้นควิเบค (Quebec's

---

[55] มาตรา 13 อนุมาตรา 3 ได้ถูกเพิ่มเติมเข้ามาเมื่อมีการปรับปรุงแก้ไขพระราชบัญญัติในปี พ.ศ.2548.

[56] อ้างถึง METI, 2006.

Consumer Protection Act) ได้กำหนดห้ามผู้ประกอบธุรกิจมิให้ทำการซื้อขายสินค้าหรือบริการกับเด็กที่มีอายุต่ำกว่า 13 ปี[57] ส่วนที่ประเทศอื่นนั้นก็มีกฎระเบียบที่มาคุ้มครองผู้เยาว์จากการเข้าใช้บริการเนื้อหา (Content) บางประเภท อย่างในประเทศออสเตรเลีย ฟินแลนด์ เยอรมัน เกาหลี แมกซิโก สาธารณรัฐสโลวัก และประเทศสวิสเซอร์แลนด์ ซึ่งประมวลกฎหมายอาญาของประเทศสวิสเซอร์แลนด์ (Switzerland's Penal Code) ได้ห้ามจำหน่ายสื่อลามกต่างๆแก่ผู้เยาว์ (ที่มีอายุ 16 ปีหรือต่ำกว่านั้น)[58] หรือในพระราชบัญญัติว่าด้วยข้อกำหนดทางอาญา พ.ศ.2538 (Australia's Criminal Code Act 1995) ได้กำหนดห้ามมิให้ส่งหรือรับภาพลามกอนาจารของเด็ก (child pornography) และส่งสื่อลามกต่างๆให้แก่บุคคลที่มีอายุต่ำกว่า 16 ปี เพื่อวัตถุประสงค์ในการดึงดูดความสนใจของเด็ก[59] หรือในประเทศแมกซิโกก็ได้มีการนำกฎหมายสหพันธรัฐว่าด้วยการคุ้มครองผู้บริโภค (Federal Law of Consumer Protection: LFPC) มาตรา 76 ทวิ มาปรับใช้กับ

---

[57] ตามมาตรา 248 ใน: <www.canlii.org/qc/laws/sta/p-40.1/20060115/whole.html>.

[58] ตามมาตรา 197 ใน: <www.admin.ch/ch/f/rs/311_0/a197.html>. ในประเทศเยอรมันมาตรา 184 และ 184c แห่งประมวลกฎหมายอาญาของประเทศเยอรมัน (*Straggesetzbuch-StGB*) นั้นมุ่งคุ้มครองผู้เยาว์จากเนื้อหาลามกอนาจาร (Pornographic Content).

[59] กรมการสื่อสารมวลชน เทคโนโลยีสารสนเทศ และศิลปะ (The Department of Communications, Information Technology and the Arts) ได้พิจารณาการเข้าถึงอินเตอร์เน็ตทางโทรศัพท์เคลื่อนที่โดยผู้เยาว์และได้คัดกรองข้อกำหนดใน DCITA (2006) หน้า 106-112 นอกจากนั้นรัฐมนตรี วุฒิสมาชิก Helen Coonan ได้ประกาศในวันที่ 22 สิงหาคม พ.ศ.2549 ว่าในไม่ช้าเธอจะนำกฎหมายรัฐสภา (Parliament legislation) มาขยายความคุ้มครองผู้เยาว์เกี่ยวกับอินเตอร์เน็ต หรือโทรทัศน์ไปถึงเนื้อหา (content) ที่ถูกส่งผ่านอุปกรณ์สื่อสารแบบผสมผสาน (convergent devices) อย่างเช่น โทรศัพท์เคลื่อนที่ในปัจจุบัน กฎหมายใหม่จะรวมการห้ามเนื้อหาประเภทสำหรับผู้ใหญ่ เช่นเดียวกันกับข้อกำหนดสำหรับผู้บริโภคว่าด้วยคำแนะนำ และการกำหนดอายุในการเข้าถึงเนื้อหา (content) ที่เหมาะสมสำหรับผู้ใหญ่เท่านั้น ข้อห้ามนี้จะมีการกำหนดโทษกรณีฝ่าฝืนกรอบการกำกับดูแลใหม่นี้ ซึ่งรวมถึงโทษทางอาญาสำหรับการกระทำผิดกฎหมายร้ายแรง ตาม <www.minister.dcita.gov.au/media/media_releases/content_safeguards_extended_to_mobile_phones>.

กรณีนี้ด้วย โดยเงื่อนไขที่ตั้งขึ้นที่กำหนดให้ผู้ให้บริการจะต้องหลีกเลี่ยงการใช้แผนการขายหรือการโฆษณาที่ไม่ได้ให้ความชัดแจ้งแก่ผู้บริโภค และไม่ได้ให้ข้อมูลที่เพียงพอเกี่ยวกับบริการที่เสนอมา โดยเฉพาะอย่างยิ่ง ในกรณีของการซื้อขายสินค้าหรือบริการที่มุ่งกระทำต่อบุคคลที่มีความเปราะบาง (vulnerable person) เช่น เด็ก คนชรา และคนป่วย รวมไปถึงวิธีการให้คำแนะนำแก่พวกเขาเมื่อข้อมูลสารสนเทศดังกล่าวไม่เหมาะสมกับคนกลุ่มนี้

ระเบียบแนวทางในการกำกับดูแล (Regulatory guidelines) ยังสามารถใช้ควบคุมการบริการเนื้อหา (Content) ได้อีกด้วย ตัวอย่างคือ กลุ่มพิทักษ์สิทธิผู้บริโภคของฟินแลนด์ (Finland's Consumer Ombudsman) ได้ออกคู่มือสำหรับบริการที่มีกลุ่มเป้าหมายเป็นผู้เยาว์[60] (guidelines for services targeting minors) โดยอยู่บนพื้นฐานของข้อบังคับการตลาดและการทำสัญญา (marketing and contract terms) ในพระราชบัญญัติว่าด้วยการคุ้มครองผู้บริโภค (Consumer Protection Act) ได้ระบุว่าหากในหน้าอินเตอร์เน็ต (internet) สำหรับกลุ่มเป้าหมายที่เป็นผู้เยาว์นั้นมีฟังก์ชั่นหรือข้อมูลที่ไม่เหมาะสมสำหรับเด็กหรือเยาวชนจะต้องถูกลบออกไป โดยคู่มือ (guidelines) ได้กำหนดว่า ควรจะมีการแยกข้อมูลที่เหมาะสมกับเฉพาะผู้ใหญ่ ออกจากเว็บไซต์ (websites) สำหรับเด็กหรือเยาวชนอย่างชัดเจน ในการตัดสินคดีในต้นปี พ.ศ.2547 กลุ่มพิทักษ์สิทธิผู้บริโภค (ombudsman) สามารถบรรลุข้อตกลงกับผู้ให้บริการให้ส่งข้อความทางโทรศัพท์เคลื่อนที่สำหรับผู้เยาว์ในการสร้างข้อกำหนดรายสัปดาห์ และแจ้งแก่ผู้ปกครองผ่านทางไปรษณีย์อิเล็กทรอนิกส์ (e-mail) ว่าบุตรหลานของตนได้ขอใช้บริการดังกล่าว ในประเทศนอรเวย์คู่มือของกลุ่มพิทักษ์สิทธิผู้บริโภคว่าด้วยบริการเนื้อหาทางโทรศัพท์เคลื่อนที่ (CO guidelines) ก็ได้มีการกำหนดถึงในประเด็นนี้เช่นกัน[61]

การกำกับดูแลตนเองในส่วนของเนื้อหาทางโทรศัพท์เคลื่อนที่ (Self-regulation of Mobile content) ก็ได้มีการนำมาใช้อย่างแพร่หลายในประเทศสมาชิกขององค์การเพื่อความ

---

[60] คู่มือของกลุ่มพิทักษ์สิทธิผู้บริโภค (Consumer Ombudsman's guidelines) (ผู้เยาว์ (minors) การซื้อขายสินค้าหรือบริการ (marketing) และการซื้อ (purchases)) ดูข้อมูลเพิ่มเติมได้ที่ <www.kuluttajavirasto.fi/user/loadFile.asp?id=5603>.

[61] ข้อ 4.1 กำหนดว่าบริการเนื้อหาทางโทรศัพท์เคลื่อนที่ (Mobile content services) จะต้องไม่เสนอต่อเด็กหรือบุคคลที่อายุน้อย หากว่าเนื้อหานั้นไม่เหมาะสมสำหรับกลุ่มอายุ (เช่น สยองขวัญ (frightening) รุนแรง (violent) กระตุ้นความรู้สึกทางเพศ (erotic) หรือลามกอนาจาร (pornographic)) ข้อที่ 4.2 กล่าวถึงการเปิดเผยข้อมูลเกี่ยวกับการจำกัดอายุ ดูข้อมูลเพิ่มเติมได้ที่ <www.forbrukerombudet.no/asset/1656/1/1656_1.pdf>.

ร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development: OECD) ตัวอย่างเช่น แนวปฏิบัติของสภาหอการค้าระหว่างประเทศ (ICC's code of conduct) เกี่ยวกับการคุ้มครองผู้เยาว์ ข้อที่ 18 และ D7 ในขณะที่พวกเขาไม่ได้มีการกำหนดขอบเขตไปถึงการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (m-commerce) แต่ก็ได้มีการกำหนดว่าควรจะใช้การดูแลเป็นพิเศษเมื่อมีการซื้อขายสินค้าหรือบริการกับเด็ก (children) หรือบุคคลที่มีอายุน้อย (young people) หรือที่มีเด็กหรือบุคคลที่มีอายุน้อยเป็นกลุ่มเป้าหมาย[62] ในสหราชอาณาจักรผู้ให้บริการโทรศัพท์เคลื่อนที่ได้จัดการกับปัญหานี้โดยการใช้แนวปฏิบัติว่าด้วยเนื้อหา (Code of practice on content)[63] สำหรับเนื้อหาทางการค้า (commercial content) เช่น หนัง เกมต่างๆ ยกเว้นบริการเสริมเสียงหรือข้อความต่างๆ (premium rate voice or texting services) จะเป็นไปตามกรอบการพัฒนาโดย Independent Mobile Classification Body (IMCB) ส่วนบริการเสริมเสียงหรือข้อความ (premium voice or texting services) นั้นทำงานภายใต้แนวปฏิบัติของคณะกรรมการอิสระกำกับดูแลมาตรฐานของบริการข้อมูลทางโทรศัพท์ (ICSTIS Code of Practice) ซึ่งสำนักงานการสื่อสาร (Office of Communications: Ofcom) ได้บัญญัติกฎหมายที่สนับสนุนการทำงานของคณะกรรมการอิสระกำกับดูแลมาตรฐานของบริการข้อมูลทางโทรศัพท์ (Independent Committee for Supervision of Standards of Telephone Information Services: ICSTIS) โดยกำหนดว่า ผู้ให้บริการโทรศัพท์เคลื่อนที่แต่ละรายต้องจัดแยกชนิดของเนื้อหา (Content) เป็น "18" (หมายถึง สิ่งที่ไม่เหมาะสมสำหรับผู้เยาว์) นอกเหนือจากการควบคุมการเข้าถึง และทำให้มันปรากฏต่อผู้บริโภคเฉพาะในกรณีเมื่อได้มีการพิสูจน์จนเป็นที่พอใจแล้วว่าผู้บริโภคนั้นมีอายุครบ 18 ปี หรือมากกว่านั้นแล้ว ในทางกลับกัน เนื่องจากผู้ให้บริการโทรศัพท์เคลื่อนที่ (mobile operators) ไม่ได้มีการควบคุมเนื้อหา (Content) ที่ถูกเสนอบน

---

[62] โดยเฉพาะอย่างยิ่ง ได้กำหนดว่า สินค้าที่ไม่เหมาะสมสำหรับเด็กหรือบุคคลที่อายุน้อยไม่ควรที่จะถูกโฆษณาในสื่อที่มีกลุ่มเป้าหมายเป็นเด็กหรือบุคคลที่อายุน้อย และการโฆษณาที่ถูกส่งตรงไปยังเด็กหรือบุคคลที่อายุน้อยไม่ควรสอดแทรกในสื่อที่มีเนื้อหาที่ไม่เหมาะสมสำหรับพวกเขา, ดูข้อมูลเพิ่มเติมได้ที่ <www.iccwbo.org/policy/marketing/id8532/index.html>.

[63] แนวปฏิบัติในการกำกับดูแลตนเองสำหรับเนื้อหา (Content) บนโทรศัพท์เคลื่อนที่ในรูปแบบใหม่ๆ ของสหราชอาณาจักร (UK Code of Practice for the Self-regulation of New Forms of Content on Mobiles) วันที่ 19 มกราคม 2547 โดย O2 (UK), Orange Personal Communications Services, T-Mobile UK, Virgin Mobile Telecoms, Vodafone และ Hutchison 3G UK.

อินเตอร์เน็ต (internet) แนวการปฏิบัติ (code) จึงได้มีการแนะนำให้นำการคัดกรองมาปรับใช้กับบริการทางอินเตอร์เน็ต (Internet access service) ท้ายที่สุดสำหรับกรณีของเนื้อหาที่ผิดกฎหมาย (illegal content) แนวการปฏิบัติ (code) ได้ชี้แนะว่ามันจะต้องถูกรายงานถึงบริษัทกฎหมาย (law enforcement agencies) นอกจากนี้ ถ้าเนื้อหา (Content) ดังกล่าวอยู่ในพื้นที่ที่ผู้ให้บริการโทรศัพท์เคลื่อนที่ (mobile operators) สามารถควบคุมได้ ก็สมควรที่จะถูกดำเนินคดีโดยเป็นไปตามข้อกำหนดที่ได้ “แจ้ง (notify) หรือจดบันทึก (take-down)” เอาไว้

แนวการปฏิบัติของสหราชอาณาจักร (United Kingdom’s code of practice) ก็ได้มีการระบุถึงการคัดกรองเนื้อหา (Content) ซึ่งครอบคลุมไปถึงเนื้อหา (Content) ชนิดใหม่ๆ รวมไปถึง visual content การพนันออนไลน์ (online gambling) การเล่นเกมผ่านทางโทรศัพท์เคลื่อนที่ (mobile gamine) ห้องสนทนาต่างๆ (chat rooms) และการเข้าอินเตอร์เน็ต (Internet access) ยกตัวอย่างเช่น ผู้ให้บริการได้จัดแบ่งหมวดหมู่ของเนื้อหา (Content) ทางการพาณิชย์ของผู้ให้บริการ และจัดเตรียมระบบการคัดกรอง (filtering systems) ให้แก่ผู้ปกครองที่จะสามารถติดตั้งการคัดกรอง (filtering function) ในหน้าอินเตอร์เน็ต (internet sites) สำหรับเด็กในความปกครองของพวกเขา อีกทั้ง ยังได้มีการตั้งกลุ่มอิสระ (independent body) เพื่อตั้งมาตรฐานในการจัดหมวดหมู่ของเนื้อหา (Content) จัดหาคำแนะนำให้แก่ผู้ให้บริการเนื้อหา (Content providers) และจัดการกับการร้องเรียนในเรื่องการจัดหมวดหมู่เนื้อหา (Content) ที่ผิดพลาด ในประเทศเดนมาร์ก ได้มีกรอบความตกลงสำหรับบริการเนื้อหาผ่านทางโทรศัพท์เคลื่อนที่ (framework agreement for mobile content services) ซึ่งถูกสร้างขึ้นโดยผู้ประกอบกิจการโทรคมนาคมของประเทศ (country’s telecommunication operators)[64] ซึ่งผู้ให้บริการ (service providers) จะต้องปฏิบัติตามข้อตกลงและใช้ associated application codes เมื่อเสนอบริการเนื้อหาผ่านทางโทรศัพท์เคลื่อนที่ (mobile content services) กระทรวงกิจการภายในประเทศและการสื่อสารของญี่ปุ่น (Japan’s Ministry of Internal Affairs and Communications: MIC) ได้มีการพิจารณาเทคโนโลยีการคัดกรอง (filtering technology) ซึ่งเหมาะสมกับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (mobile commerce) โดยเฉพาะมาตั้งแต่ปี พ.ศ. 2547

ในประเทศเยอรมัน เพื่อปกป้องคุ้มครองผู้เยาว์จากสิ่งที่ผิดกฎหมาย สื่อลามก หรือเนื้อหา (Content) อื่นๆที่มีอันตรายอย่างมากต่อผู้ที่มีอายุน้อย และเพื่ออนุญาตให้ผู้ปกครองขัดขวางการเข้าใช้บริการผ่านโทรศัพท์เคลื่อนที่ของเด็ก ผู้ให้บริการโทรศัพท์เคลื่อนที่รายใหญ่ทุกราย (all major mobile carriers) นั้นได้มีการสร้างแนวปฏิบัติร่วมกัน (joint code of conduct)

---

[64] <www.teleindu.dk/t2w_358.asp>.

ตัวอย่างเช่น พวกเขาตกลงที่จะจัดระบบการตรวจสอบอายุ (age verification system)[65] ยิ่งไปกว่านั้น มีการนำสนธิสัญญาระหว่างรัฐว่าด้วยการคุ้มครองสื่อสำหรับผู้เยาว์ (Youth Media Protection Interstate Treaty) (*Jugendmedienschutz- Staatsvertrag: JMStV)* ซึ่งจะมีผลใช้บังคับในเดือนเมษายน พ.ศ.2546 มาปรับใช้กับเนื้อหาผ่านทางโทรศัพท์เคลื่อนที่ (mobile content) องค์กรหลักในการควบคุม (main supervisory organizations) คือ คณะกรรมการคุ้มครองผู้เยาว์จากสื่อที่มีเนื้อหาไม่เหมาะสม (Commission for the Protection of Minors from Unsuitable Media Content) (***Kommission für Jugendmedienschutz*** – KJM) และองค์กรการกำกับดูแลตนเองโดยสมัครใจ (voluntary self-regulatory organisations) (SKEs) ที่มีการรับรองโดยคณะกรรมการคุ้มครองผู้เยาว์จากสื่อที่มีเนื้อหาไม่เหมาะสม (KJM) ในประเทศสหรัฐอเมริกาได้นำ Dot Kids Implementation and Efficiency Act of 2002 มาปรับใช้เพื่อจัดให้มี "www.kids.us" ซึ่งเป็นเว็บไซต์ (website) ที่ส่งเสริมความปลอดภัยในการออนไลน์สำหรับเด็กที่มีอายุต่ำกว่า 13 ปี NeuStar มีหน้าที่สำหรับพัฒนาคู่มือ (guidelines) และการควบคุมเพื่อให้แน่ใจว่าเนื้อหา (Content) บนเว็บ Kids.us นั้นทั้ง "เหมาะสมสำหรับผู้เยาว์" และไม่ "เป็นอันตรายแก่ผู้เยาว์"

2.5.4 การให้ข้อมูลและการรณรงค์ให้ความรู้ที่เกิดขึ้น

การรณรงค์ให้ความรู้และข้อมูลข่าวสารได้ถูกใช้อย่างกว้างขวางในประเทศสมาชิกในหลายๆประเทศเพื่อให้ความคุ้มครองผู้เยาว์ ในประเทศเยอรมัน ศูนย์ให้คำปรึกษาในแคว้นธูริงเกีย (Thuringia Consumer Advice Centre) (***Verbraucher-Zenrale Thüringen e.V***) ได้สร้าง CD-ROM ชื่อ "Achtung Taschengeldgangster" สำหรับเด็กที่มีอายุ 10-12 ปี และจัดเตรียมโดยไม่คิดค่าใช้จ่ายในทุกคำปรึกษาของคณะกรรมการผู้บริโภค ศูนย์ให้คำปรึกษาในแคว้นธูริงเกีย (The

---

[65] <www.t-mobile.de/downloads/t-mobile_broschueren/t-mobile__verhaltenskodex_der_mobilfunkanbieter_in_deutschland_zum_jugendschutz_im_mobilfunk.pdf>.

อีกแนวปฏิบัติ (Code of conduct) หนึ่งซึ่งประกาศในประเทศเยอรมันในปี พ.ศ. 2546 โดยสมาคมอุตสาหกรรมบริการเสริมพิเศษ (An association of premium rate services industries) (***Verhaltenskodex des Vereins Freiwillige Selbstkontrolle Telefonmehrwert-dienste e.V.***) ซึ่งรวมถึงหลักเกณฑ์ทั่วไปของการจัดการและการแนะนำในการกำหนดอัตราค่าบริการเสริมพิเศษ (premium rate services) สำหรับสมาชิก อย่างไรก็ตาม แนวปฏิบัติไม่ได้สร้างมาตรฐานใดๆที่นอกเหนือจากบทบัญญัติแห่งกฎหมาย (statutory provisions).

Thuringia Consumer Advice Centre) ยังได้สร้างคู่มือ (booklet) เรื่องคอมพิวเตอร์ โทรศัพท์เคลื่อนที่ โทรทัศน์ และ Co. (Computer, mobile phone, TV and Co.) เพื่อจัดการกับประเด็นที่เกี่ยวกับโทรทัศน์และวีดีโอบนคอมพิวเตอร์และโทรศัพท์เคลื่อนที่ อีกทั้ง ในประเทศเยอรมัน การจัดทำหนังสือคู่มือเพื่อเผยแพร่ทั่วไป โดยทำเป็นหนังสือฉบับเล็กๆสำหรับพกพา (handy booklet) กำลังอยู่ในขั้นตอนการวางแผนโดยศูนย์ให้คำปรึกษาสำหรับคนที่เป็นหนี้ในเบอร์ลิน (Berlin debtor advice centre) กับกระทรวงโภชนาการ เกษตรและคุ้มครองผู้บริโภค (Federal Minister of Food, Agriculture and Consumer Protection: BMELV) ในประเทศโปแลนด์ ใบปลิว (information leaflet) เกี่ยวกับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (mobile commerce) และผู้บริโภคที่มีอายุน้อย (junior consumers) (“*Telefonia komórkowa a mlody konsument*”) ซึ่งถูกสร้างขึ้นโดย OCCP ในปี 2004[66] ในประเทศสวิสเซอร์แลนด์ คณะกรรมการการสื่อสารแห่งชาติ (Federal Office of Communications: OFCOM) ซึ่งมีอำนาจในการควบคุมการติดต่อสื่อสาร ได้สร้างหนังสือคู่มือ (booklet) เรื่อง “SMS messages that cost” ในเดือนมิถุนายน พ.ศ.2548 ซึ่งหนังสือเล่มนี้มุ่งให้ข้อมูลเกี่ยวกับการคุกคามที่อาจเกิดขึ้นได้ วิธีจัดการกับค่าใช้จ่าย วิธีการป้องกันการกระทำที่มิชอบ และควรที่จะติดต่อกับผู้ใดในกรณีที่เกิดปัญหาขึ้น ในประเทศฟินแลนด์ บ่อยครั้งที่ตัวแทนผู้บริโภค (Consumer Agency) ได้เสนอข้อมูลเกี่ยวกับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (mobile commerce) ลงในนิตยสารชื่อ KULUTTAJA และในเว็บไซต์ (website) ของพวกเขา ในฐานะโครงการร่วมกัน (joint project) กลุ่มพิทักษ์สิทธิผู้บริโภคแห่งประเทศในแถบสแกนดิเนเวีย (Nordic ombudsmen) ออกเกมออนไลน์ที่เรียกว่า “Nordic Galactor” ในปีพ.ศ.2550 เพื่อสอนเด็กและวัยรุ่นเกี่ยวกับหลักการที่สำคัญและความเสี่ยงต่างๆที่เกี่ยวกับการพาณิชย์อิเล็กทรอนิกส์และการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (electronic and mobile commerce) และการบริการข้อมูลอื่นๆแก่ชุมชน (other information society services) ในประเทศออสเตรเลีย คณะกรรมการเพื่อผู้บริโภคและการแข่งขันของออสเตรเลีย (Australian Competition and Consumer Commission : ACCC) ได้จัดให้มีข้อแนะนำเกี่ยวกับการพาณิชย์ผ่านทางโทรศัพท์เคลื่อนที่ (mobile commerce tips) บนเว็บไซต์ (website) ให้แก่ผู้บริโภค[67]

---

[66] ในเวอร์ชั่น 2006 ฉบับภาษาโปแลนด์, ดูข้อมูลเพิ่มเติมได้ที่ <www.uokik.gov.pl/download/Z2Z4L3Vva2lrL3BsL2tzZ19weXRhbmlhLnYwLzEzMC8yMS8xL3RlbGVmb25pYV9rb21vcmtvd2EucGRm>.

[67] <www.accc.gov.au/content/index.phtml/itemId/266899/fromItemId/8135>.

บริษัทเอกชน (Private companies) และองค์กรภาคอุตสาหกรรม (industry organizations) ได้เข้ามามีส่วนในการพัฒนาใบปลิว ยกตัวอย่างเช่น สถาบันครอบครัวและผู้ปกครองแห่งชาติ (National family and parenting institute) ในสหราชอาณาจักรได้ร่วมกับ Vodafone สร้างคู่มือสำหรับผู้ปกครอง[68] ในประเทศออสเตรเลีย นอกจากคู่มือของรัฐสำหรับเยาวชน (government's guide for youth) ซึ่งตีพิมพ์ออกมาในเดือนกันยายน พ.ศ.2546[69] ยังมีชมรมยุวอาสากาชาดออสเตรเลีย (Austrian Red Cross Youth) และกลุ่มนักกฎหมาย (***Kinder- und Jugendanwaltschaft Wien***) ร่วมกับ Mobilkom Austria จัดทำใบปลิวสำหรับเด็ก[70] ในประเทศออสเตรเลีย มี NetAlert ซึ่งเป็นอินเตอร์เน็ตที่ได้รับเงินอุดหนุนจากรัฐโดยมีเนื้อหาเป็นการให้ข้อมูลความรู้เพื่อความปลอดภัยเกี่ยวกับ "mobile Internet enhanced devices" แก่ผู้ปกครอง[71] Australian Interactive Media Industry Association (AIMIA) ก็ได้มีการเริ่มรณรงค์ให้ความรู้แก่ผู้บริโภคที่ใช้บริการเนื้อหา (Content) บนโทรศัพท์เคลื่อนที่ทางโทรทัศน์ และลงในแผ่นพับโฆษณาต่างๆ ในเว็บไซต์ และในหน้าจอโทรศัพท์เคลื่อนที่เพื่อที่จะให้แน่ใจว่าผู้บริโภคได้มีประสบการณ์ที่ดีกับบริการเนื้อหา (Content) บนโทรศัพท์เคลื่อนที่[72] ในประเทศญี่ปุ่นภาคอุตสาหกรรมได้ร่วมมือกับคณะรัฐมนตรีสร้าง "E-net Caravan" ซึ่งมีการบรรยายที่สอนวิธีการใช้อินเตอร์เน็ตและโทรศัพท์เคลื่อนที่อย่างปลอดภัยและด้วยความมั่นใจให้แก่ผู้ปกครองและครูอาจารย์ต่างๆ[73]

---

[68] <www.family-parenting.org/Bullying/StayingInTouch-ParentsGuide.pdf>.

[69] "Der Handy-Guide-Alles was Recht ist" โดย Federal Ministry of Social Security, Generations and comsumer Protection (BMSGK), ดูข้อมูลเพิ่มเติมได้ที่ <www.bmsg.gv.at/cms/site/attachments/2/9/3/CH0036/CMS1091089868037/handybroschuerear5.pdf> (ภาษาเยอรมัน).

[70] "Handy Guide – Alles rund ums Telefonieren mit dem Handy" (ภาษาเยอรมัน), ดูข้อมูลเพิ่มเติมได้ที่ <www.mobilkomaustria.com/CDA/getAttachment_mk/0,3148,1048,00.handy_guide.pdf>

[71] <www.netalert.net.au/02349-Mobile-Internet-Enabled-Devices.pdf>.

[72] ลงวันที่ 31 สิงหาคม 2549, ดูข้อมูลเพิ่มเติมได้ที่ <www.aimia.com.au/i-cms?page=2299>.

[73] <www.fmmc.or.jp/e-netcaravan/> (ภาษาญี่ปุ่น).

ดังนั้น ในประเด็นการคุ้มครองผู้เยาว์ ได้มีการกำหนดว่า เด็กอายุต่ำกว่า 7 ปี ไม่มีความสามารถเพียงพอที่จะทำสัญญาได้ หากทำสัญญานั้นเป็นโมฆะ ในขณะที่บุคคลที่อายุต่ำกว่า 18 ปี จะถูกจำกัดความสามารถตามกฎหมาย สามารถที่จะเข้าทำได้แต่เฉพาะธุรกรรมทั่วไปที่ไม่ก่อให้เกิดผลใดๆมากนัก ไม่มีสิทธิในการก่อหนี้ และอาจเข้าทำสัญญาได้ในกรณีที่ได้รับความยินยอมจากผู้ปกครอง และบังคับให้บิดามารดาหรือผู้ปกครองตามกฎหมายมีสิทธิและหน้าที่ที่จะต้องรับผิดชอบต่อการกระทำทางกฎหมายของเด็กที่อยู่ในความปกครอง ทั้งต้องกำหนดให้ผู้ประกอบธุรกิจต้องกำหนดเพดานการให้บริการแต่ละอย่างในกลุ่มเป้าหมายที่เป็นผู้เยาว์ และจะต้องจัดให้มีบริการที่เป็นธรรมและเป็นไปตามกฎหมายเมื่อกลุ่มเป้าหมายทางธุรกิจของพวกเขาเป็นผู้เยาว์ แม้ว่าบิดามารดามีหน้าที่ตามกฎหมายอย่างผู้ปกครองแล้วก็ตาม และต้องแจ้งรายละเอียดต่อผู้เยาว์ว่า สัญญาสามารถทำการยกเลิกได้โดยผู้เยาว์หรือผู้ปกครอง ถ้าผู้ปกครองไม่ได้ให้ความเห็นชอบในการเข้าทำสัญญาดังกล่าว ทั้งต้องดำเนินการทุกขั้นตอนอย่างเหมาะสมเพื่อป้องกันผู้เยาว์ทำธุรกรรมทางการเงิน และกำหนดให้โปรแกรมรวบรวมข้อมูล (Aggregator) ต้องยืนยันได้ว่า ผู้ใช้แต่ละคนมีอายุตามที่กฎหมายในแต่ละท้องถิ่นกำหนด ก่อนที่จะอนุญาตให้ผู้ใช้ดังกล่าวเข้าร่วมในโปรแกรมหรือรับข้อความ มาตรการอีกอย่างคือการใช้หมายเลขรหัสบุคคล (PIN) ในการควบคุมการเข้าใช้บริการเนื้อหา (Content) สำหรับผู้ใหญ่ของเด็ก อย่างเช่น บริการลามกทางโทรศัพท์ (telephone sex) รวมไปถึงการพิสูจน์อายุเพื่อให้แน่ใจว่าเด็กไม่ได้เข้าใช้บริการสำหรับผู้ใหญ่ ผู้ประกอบกิจการโทรศัพท์เคลื่อนที่ (Mobile phone operators) ต้องห้ามมิให้ส่งบริการหรือเสนอบริการสำหรับผู้ใหญ่แก่ผู้เยาว์ และต้องมีวิธีการควบคุมโทรศัพท์เคลื่อนที่ของผู้เยาว์ที่มีอายุต่ำกว่า 18 ปีที่ได้จดทะเบียนไว้ ทำให้โทรศัพท์เคลื่อนที่เครื่องนั้นไม่สามารถที่จะเข้าใช้บริการสำหรับผู้ใหญ่ได้ ผู้ให้บริการจะต้องหลีกเลี่ยงการใช้แผนการขายหรือการโฆษณาที่ไม่ได้ให้ความชัดแจ้งแก่ผู้บริโภค และไม่ได้ให้ข้อมูลที่เพียงพอเกี่ยวกับบริการที่ถูกเสนอมาโดยเฉพาะอย่างยิ่ง ในกรณีของการซื้อขายสินค้าหรือบริการที่มุ่งกระทำต่อบุคคลที่มีความเปราะบาง เช่น เด็ก คนชรา และคนป่วย รวมไปถึงวิธีการให้คำแนะนำเมื่อข้อมูลสารสนเทศดังกล่าวไม่เหมาะสมกับพวกเขา และควรจะมีการแยกข้อมูลที่เหมาะสมกับเฉพาะผู้ใหญ่ ออกจากเว็บไซต์ (websites) หรือบริการสำหรับเด็กหรือเยาวชนอย่างชัดเจน ทั้งสร้างข้อกำหนดรายสัปดาห์ และแจ้งแก่ผู้ปกครองผ่านทางไปรษณีย์อิเล็กทรอนิกส์ (e-mail) หรือข้อความสั้น (SMS) ว่าบุตรหลานของตนได้ขอใช้บริการดังกล่าว ผู้ให้บริการโทรศัพท์เคลื่อนที่แต่ละรายต้องจัดแยกชนิดของเนื้อหา (Content) นอกเหนือจากการควบคุมการเข้าถึง และทำให้มันปรากฏต่อผู้บริโภคเฉพาะในกรณีเมื่อได้มีการพิสูจน์จนเป็นที่พอใจแล้วว่าผู้บริโภคนั้นมีอายุครบ 18 ปี หรือมากกว่า

นั้นแล้ว และจัดเตรียมระบบการคัดกรอง (filtering systems) ให้แก่ผู้ปกครองที่จะสามารถติดตั้งการคัดกรอง (filtering function) ในหน้าอินเตอร์เน็ต (internet sites) และหน้าจอโทรศัพท์เคลื่อนที่ สำหรับเด็กในความปกครองของพวกเขา และตั้งหน่วยงานอิสระ เพื่อตั้งมาตรฐานในการจัดหมวดหมู่ของเนื้อหา (Content) และจัดหาคำแนะนำให้แก่ผู้ให้บริการเนื้อหา (Content providers) ในกรณีของเนื้อหาที่ผิดกฎหมาย จะต้องรายงานต่อตัวแทนที่บังคับใช้กฎหมาย นอกจากนี้ ถ้าเนื้อหา (Content) ดังกล่าวอยู่ในพื้นที่ที่ผู้ให้บริการโทรศัพท์เคลื่อนที่ (mobile operators) สามารถควบคุมได้ ก็สมควรที่จะถูกดำเนินคดีโดยเป็นไปตามที่กฎหมายกำหนดเอาไว้ ที่สำคัญ บริษัทเอกชน ภาคอุตสาหกรรม และภาครัฐต้องจัดให้มีการรณรงค์ให้ความรู้แก่ผู้ปกครองและผู้บริโภคที่ใช้บริการบนโทรศัพท์เคลื่อนที่ทางโทรทัศน์ และลงในแผ่นพับโฆษณาต่างๆ ในเว็บไซต์ และในหน้าจอโทรศัพท์เคลื่อนที่ รวมทั้งแจกจ่ายคู่มือให้คำแนะนำแก่ผู้ปกครองและผู้บริโภค

2.6 ประเด็นความเป็นส่วนตัว (Privacy)

2.6.1 ประเด็นเรื่องความเป็นส่วนตัวที่เพิ่มมากขึ้นจากการให้บริการระบุพิกัดตำแหน่ง (Location-based services)

เทคโนโลยีที่แตกต่างกันได้ถูกพัฒนาเพื่อระบุตำแหน่งของโทรศัพท์เคลื่อนที่ (mobile phone's location) เทคโนโลยีเหล่านี้สามารถแบ่งออกเป็นสามกลุ่มใหญ่ๆด้วยกันคือ หนึ่ง โทรศัพท์เคลื่อนที่สามารถคำนวณตำแหน่งตัวเองได้ (GPS) สองคือ เครือข่ายโทรศัพท์เคลื่อนที่สามารถคำนวณหาตำแหน่งได้ (Cell ID และการสำรวจที่ตั้งของผู้ใช้บริการ (subscriber)) และสามคือ การผสมกันของเทคนิคต่างๆ 2 อย่างหรือกว่านั้นขึ้นไป เพื่อสนับสนุนระบบระบบบอกพิกัดผ่านทางดาวเทียม (Global Positioning System: GPS) [74] ผู้ให้บริการด้านเครือข่าย (network operators) ในบางประเทศได้เริ่มปรับปรุงเครือข่ายของตัวเองอันเป็นผลมาจากแรงผลักดันทางกฎหมายเพื่อให้มีความแม่นยำในเรื่องการระบุตำแหน่งมากขึ้นสำหรับใช้ในบริการกรณีฉุกเฉิน (emergency services)[75] ตัวอย่างที่เห็นได้ชัดคือ ผู้ที่ให้บริการระบบไร้สายในสหรัฐอเมริกา

---

[74] อ้างถึง Steinfield, 2004.

[75] ในสหราชอาณาจักรนั้นอยู่ภายใต้ Wireless Communications and Public Safety Act (911 Act) (1999) ในประเทศเกาหลีนั้นอยู่ภายใต้ Act on Disaster Preparedness & Safety Management มาตรา 3s. (7) และ Act on Protection and Use of Location-Based

(United States wireless carriers) ส่วนใหญ่มีความต้องการที่จะระบุตำแหน่งของผู้โทรเข้า (caller's location) ภายในระยะ 50 -300 เมตรให้ได้[76]

การพัฒนาของเทคโนโลยีการค้นหาตำแหน่ง (location-tracking technology) และระบบเครือข่ายเซ็นเซอร์ (sensor networking) ทำให้การให้บริการระบุตำแหน่ง (location information services) เป็นไปได้จริง ความสามารถในการระบุตำแหน่งของโทรศัพท์เคลื่อนที่อย่างแม่นยำทำให้การระบุตำแหน่งของผู้ใช้บริการ (individual subscriber) ได้ผลจริง ซึ่งผู้ใช้บริการโทรศัพท์เคลื่อนที่ (mobile phone users) ส่วนมากเป็นปัจเจกบุคคล (***individuals***) ผลที่ตามมาก็คือ ข้อมูลตำแหน่งที่ตั้ง (location information) จะถูกพิจารณาให้กลายเป็นข้อมูลส่วนบุคคลและถูกจัดอยู่ในขอบเขตการคุ้มครองของกฎหมายข้อมูลส่วนบุคคล (privacy laws)

ก่อนหน้านี้ ข้อมูลการระบุตำแหน่ง (location information) ถูกสร้างขึ้นเพื่อใช้ในการก่อให้เกิดและคงไว้ซึ่งการเชื่อมต่อกับโทรศัพท์เคลื่อนที่เท่านั้น ดังนั้น ข้อมูลการระบุตำแหน่งจะเกี่ยวข้องกับผู้ให้บริการเครือข่ายโทรคมนาคม (operators of telecommunications networks) เท่านั้น ซึ่งมักจะถูกจำกัดขอบเขตโดยตัวบทกฎหมายข้อมูลส่วนบุคคลด้านโทรคมนาคม (Telecommunications privacy legislation)[77] อย่างไรก็ตาม การพัฒนาการพาณิชย์ทางโทรศัพท์เคลื่อนที่ (mobile commerce) ได้นำไปสู่การสร้างสรรค์บริการอันหลากหลายบนพื้นฐานความรู้เกี่ยวกับตำแหน่งที่ถูกต้องของผู้ใช้บริการ (user's precise location) ดังนั้น การให้บริการระบุพิกัดตำแหน่ง (location-based information services) โดยใช้เทคโนโลยีบอกพิกัดผ่านทางดาวเทียม (Global Positioning System: GPS) และระบบเครือข่ายเซ็นเซอร์อื่น (other sensor networks) จะเป็นตัวก่อให้เกิดโอกาสที่สำคัญในการพาณิชย์ทางโทรศัพท์เคลื่อนที่ (mobile commerce)

นอกจากนี้ ปัจจุบันยังมีการให้บริการข้อมูลตำแหน่งต่างๆ (location-based services) ที่ผู้ใช้บริการ (user) ไม่จำเป็นต้องร้องขอ ที่เห็นได้ชัดคือการโฆษณาโดยใช้ข้อมูลตำแหน่ง (Location-based advertising) ที่ผู้ให้บริการจะส่งข้อความไปยังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการ ยกตัวอย่างเช่น การส่งข้อเสนอพิเศษของร้านอาหารและร้านค้าที่อยู่ในบริเวณ

Services มาตรา 29 และในสหภาพยุโรปนั้นอยู่ภายใต้ Universal Service Directive [Directive 2002/22/EC] มาตรา 26.

[76] ภายใต้ phase 2 ของ FCC's "Enhanced 911" Rules, ดูข้อมูลเพิ่มเติมได้ที่ <www.fcc.gov/911/enhanced>.

[77] อย่างในประเทศออสเตรเลีย ในส่วนที่ 13 ของ Telecommunications Act 1997.

ใกล้เคียงกับที่ตำแหน่งผู้ใช้บริการไปยังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการเหล่านั้น ซึ่งในกรณีดังกล่าว ผู้ใช้บริการบางท่านอาจมองว่าเป็นประโยชน์ ในขณะที่บางท่านอาจมองว่าเป็นการคุกคามความเป็นส่วนตัว

ดังนั้น จึงอาจเป็นประโยชน์อย่างมากหากมีการบ่งชี้ถึงองค์ประกอบหลักในการคุ้มครองความเป็นส่วนตัวในเรื่องข้อมูลตำแหน่งของผู้ใช้บริการไปพร้อมๆกับการพัฒนาเรื่องการให้บริการระบุพิกัดตำแหน่ง (location-based services) การยอมรับกฎและหลักการว่าข้อมูลตำแหน่งมีการจัดเก็บอย่างไร มีการนำข้อมูลไปใช้อะไรบ้าง และ จะสามารถเก็บข้อมูลไว้ได้นานเท่าไหร่ จะนำไปสู่การคุ้มครองความเป็นส่วนตัวของผู้ใช้บริการโทรศัพท์เคลื่อนที่

2.6.2 การได้รับความยินยอม

ความยินยอมกลายเป็นประเด็นสำคัญในเรื่องความเป็นส่วนตัวที่ถูกหยิบยกขึ้นมา อันเป็นผลมาจากการพัฒนาของการให้บริการระบุพิกัดตำแหน่ง (location-based services) คำถามที่เกิดขึ้นก็คือ ความยินยอมแบบใดที่ผู้ให้บริการควรจะต้องได้รับก่อนที่จะดำเนินการใดๆ กับข้อมูลตำแหน่งของผู้ใช้บริการโทรศัพท์เคลื่อนที่ คำถามนี้มีความสำคัญเป็นอย่างยิ่งสำหรับการดำเนินธุรกิจที่เกี่ยวข้องกับการโฆษณาโดยใช้ข้อมูลตำแหน่ง (Location-based advertising)

แนวการปฏิบัติด้านการคุ้มครองความเป็นส่วนตัวขององค์กรความร่วมมือและพัฒนาทางเศรษฐกิจ (OECD Privacy Guidelines) (ในย่อหน้าที่ 7) ได้แนะนำว่า ข้อมูลส่วนบุคคล (personal data) อันรวมถึงข้อมูลตำแหน่งของผู้ใช้บริการโทรศัพท์เคลื่อนที่ (location information for mobile users) ควรจะถูกจัดเก็บในสถานที่ที่เหมาะสมกับความรู้หรือความยินยอมของเจ้าของข้อมูลนั้นๆ

กลุ่มเจรจาผู้บริโภคสองฟากฝั่งมหาสมุทรแอตแลนติก (Trans-Atlantic Consumer Dialogue: TACD) ได้แนะแนวทางการแก้ไขในเรื่องการพาณิชย์ทางโทรศัพท์เคลื่อนที่ (mobile commerce) ไว้ว่า การใช้ข้อมูลส่วนบุคคลใดใดก็ตามซึ่งอาจรวมถึงข้อมูลตำแหน่ง โดยที่ผู้บริโภคไม่ได้ให้ความตกลงไว้โดยชัดแจ้งสมควรที่จะถูกห้าม[78] กลุ่มคณะทำงานระหว่างประเทศว่าด้วยการคุ้มครองข้อมูลทางโทรคมนาคม (International Working Group on Data Protection in Telecommunications) ได้ให้คำแนะนำที่เป็นไปในแนวทางเดียวกันคือ ผู้ใช้ยังคงต้องอยู่ความ

[78] อ้างถึง TACD, 2005.

ควบคุมของ The generation of precise location information[79] ซึ่งแนะนำว่าการให้ข้อมูลตำแหน่ง (location information) สามารถทำได้ในลักษณะที่เป็นบริการเสริม (value added services) เฉพาะเมื่อผู้ใช้บริการได้ให้ความยินยอมในเรื่องดังกล่าวอย่างชัดแจ้ง

หลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่เรียกว่าหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล (Directive on Privacy and Electronic Communications) ใน มาตรา 9 กำหนดว่า สำหรับข้อกำหนดของบริการระบุพิกัดตำแหน่ง (provision of location-based services) ให้แสดงความยินยอม (opt-in consent) ของผู้ใช้บริการ[80] และเพื่อที่จะได้รับความยินยอมจากผู้ใช้บริการ ผู้ให้บริการ (service provider) จะต้องแจ้งแก่สมาชิกว่าข้อมูลตำแหน่งประเภทไหนจะถูกนำมาใช้เพื่อวัตถุประสงค์อะไร และใช้ช่วงเวลาไหน และข้อมูลดังกล่าวจะถูกส่งไปยังบุคคลที่สามเพื่อวัตถุประสงค์ในการให้บริการอื่นอีกหรือไม่

ใน EC มาตรา 29 ว่าด้วยการประสานความร่วมมือกันระหว่างหน่วยงานด้านการคุ้มครองข้อมูล (Data Protection Working Party (2005)) ได้กำหนดเงื่อนไขที่สำคัญในการได้รับความยินยอมในเรื่องข้อมูลตำแหน่ง (location information) ภายใต้หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล (Directive) ตามที่การประสานความร่วมมือกัน (Working Party) ได้กำหนดไว้ ความยินยอมไม่สามารถถูกยกเป็นส่วนหนึ่งของข้อกำหนดและเงื่อนไขทั่วไปที่ถูกเสนอสำหรับการใช้บริการในการติดต่อสื่อสารทางระบบอิเล็กทรอนิกส์ (electronic communications) ได้

---

[79] ตั้งแต่ปี 2526 กลุ่มคณะทำงานระหว่างประเทศว่าด้วยการคุ้มครองข้อมูลทางโทรคมนาคมได้รับเอาคำแนะนำที่หลากหลาย (“Common Position” และ “Working Paper”) ซึ่งมีเป้าหมายในการปรับปรุงการคุ้มครองความเป็นส่วนตัวในการสื่อสารโทรคมนาคม ซึ่งสมาชิกของกลุ่มรวมถึงตัวแทนจากผู้มีอำนาจคุ้มครองข้อมูล (data protection authorities) และกลุ่มอื่นๆของการบริหารรัฐกิจแห่งชาติ (national public administrations) องค์กรระหว่างประเทศ (international organisations) และนักวิทยาศาสตร์ (scientists) จากทั่วโลก ดู IWGDPT (2004).

[80] Directive 2002/58/EC ของสภายุโรป (European Parliament) และของคณะกรรมการ (Council) วันที่ 12 กรกฎาคม พ.ศ.2545 เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและการคุ้มครองความเป็นส่วนตัวในส่วนของการติดต่อสื่อสารทางอิเล็กทรอนิกส์ (Directive on privacy and electronic communications) ตาม <www.europa.eu/eur-lex/pri/en/oj/dat/2002/1_201/1_20120020731en00370047.pdf>.

คณะทำงาน (Working Party) ให้ความเห็นอีกว่า การได้รับการยินยอมอาจประกอบไปด้วยข้อตกลงที่มีเงื่อนไขให้แจ้งข้อมูลเต็มรูปแบบให้แก่ผู้ใช้บริการล่วงหน้าเกี่ยวกับกระบวนการระบุตำแหน่ง ทั้งนี้ ขึ้นอยู่กับชนิดของการให้บริการ นอกจากนี้ ผู้ให้บริการเสริมจากการบริการพื้นฐานควรจะมีมาตรการที่เหมาะสมเพื่อให้แน่ใจว่าการยินยอมดังกล่าวถูกต้องตามกฎหมาย เมื่อขบวนการระบุตำแหน่งดำเนินไปอย่างต่อเนื่อง ผู้ให้บริการควรจะจัดการเรื่องนี้ให้เรียบร้อยโดยยืนยันการเป็นสมาชิกในการใช้บริการดังกล่าวโดยการส่งข้อความไปยังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการหลังจากที่ผู้ใช้บริการได้ให้ความยินยอมเป็นที่เรียบร้อยแล้ว

คณะทำงานมักจะเน้นย้ำไปที่สิทธิส่วนบุคคลของผู้ให้การยินยอมในเรื่องขบวนการระบุตำแหน่ง โดยผู้รับบริการสามารถยกเลิกการยินยอมได้ทุกเมื่อที่ต้องการภายใต้หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล (Directive on Privacy and Electronic Communications) (2002/58/EC มาตรา 9) ในบริบทของการโฆษณาโดยใช้ข้อมูลตำแหน่ง (location-based advertising)) จะสังเกตเห็นว่าหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล (Directive) จะเจาะจงไปในเรื่องการป้องกันการล่วงล้ำความเป็นส่วนตัวอันเนื่องมาจากข้อความอันไม่พึงประสงค์จากการทำการตลาดทางตรงที่ส่งมายังโทรศัพท์เคลื่อนที่ ภายใต้หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล (Directive) มาตรา 13.3 กำหนดไว้ว่า จะไม่สามารถทำการติดต่อสื่อสารอันไม่พึงประสงค์เพื่อวัตถุประสงค์ในการทำการตลาดทางตรงได้โดยปราศจากความยินยอมของผู้ใช้บริการ

ภายใต้กฎหมายสหพันธรัฐ (federal legislation) ในสหรัฐอเมริกา ข้อมูลตำแหน่งถูกพิจารณาให้เป็นเครือข่ายข้อมูลของลูกค้า (Customer proprietary network information: CPNI) และสามารถนำมาใช้ได้ก็ต่อเมื่อได้รับอนุญาตจากลูกค้าเท่านั้น เว้นแต่เกิดกรณีฉุกเฉินขึ้น[81] องค์กรประชาสังคม (Civil Society organizations: CSO) อย่างเช่น ศูนย์ประชาธิปไตยและเทคโนโลยี (Center for Democracy and Technology) ได้เรียกร้องให้คณะกรรมการกลางกำกับดูแลกิจการสื่อสารของสหรัฐเมริกา (Federal Communications Commission: FCC) ทำการชี้แจงอย่างชัดเจนในเรื่องการขออนุญาตก่อนที่จะให้บริการดังกล่าว[82]

ประเทศญี่ปุ่นและประเทศเกาหลีได้เริ่มสร้างแนวทางในการคุ้มครองการใช้ข้อมูลตำแหน่งของผู้ใช้บริการ ในประเทศญี่ปุ่น “แนวการปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจโทรคมนาคมปี 1998” (The 1998 Guidelines on the Protection of Data in

---

[81] มาตรา 222 แห่ง Communications Act (1934) ซึ่งถูกพัฒนาขึ้นโดย Wireless Communications and Public Safety Act (1999).

[82] <www.cdt.org/privacy/issues/location/020406fcc.shtml>.

telecommunications Business) มาตรา 11 กล่าวไว้ว่าบุคคลที่ทำธุรกิจเกี่ยวกับระบบโทรคมนาคมไม่ควรเปิดเผยข้อมูลตำแหน่งแก่บุคคลอื่นยกเว้นอยู่ภายใต้เงื่อนไขที่แน่นอน เช่น เมื่อเจ้าของข้อมูลนั้นได้ให้ความยินยอม[83] แนวทางที่ไม่สัมพันธ์กันเหล่านี้ ถูกรับรู้ในฐานะที่มีส่วนช่วยให้อุตสาหกรรมในญี่ปุ่นเจริญเติบโตขึ้นอย่างรวดเร็ว[84] กฎหมายคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นได้วางข้อห้ามเกี่ยวกับการใช้ข้อมูลส่วนบุคคลของผู้ใช้บริการอันรวมถึงข้อมูลตำแหน่ง และคงไว้ซึ่งการกำหนดให้ต้องได้รับความยินยอมโดยชัดแจ้งจากลูกค้าก่อนที่จะใช้ข้อมูล ตามคู่มือในปี พ.ศ.2547 (2004 guidelines)[85]

ในเดือน มีนาคม 2548 ประชากรในประเทศเกาหลีประมาณ 3.76 ล้านคนได้สมัครเป็นสมาชิกเพื่อใช้บริการระบุพิกัดตำแหน่ง[86] ทางประเทศเกาหลีเองก็พยายามหาทางปกป้องข้อมูลตำแหน่ง โดยให้ผู้ให้บริการส่งข้อความ เพื่อขอรับความยินยอมจากผู้รับบริการก่อนที่จะให้บริการต่างๆ (Act on the Promotion of Information Network Utilization and Information Protection มาตรา 50 อนุมาตรา 2) และในมาตรา 15 และ 40 ของข้อปฏิบัติเพื่อการคุ้มครองและการใช้บริการระบุพิกัดตำแหน่งของเกาหลี (Korea's new Act on the Protection and Use of Location-based Services) ได้ผลักดันให้เกิดการเรียกร้องให้มีการยินยอมจากผู้รับบริการก่อนมีการจัดเก็บ การใช้ หรือการให้ข้อมูลตำแหน่ง อีกทั้งยังมีการวางบทลงโทษทางอาญา รวมถึงระยะเวลาการจำคุก สำหรับผู้ละเมิดกฎดังกล่าว

ปัจจัยอีกตัวที่มีผลต่อความถูกต้องตามกฎหมายในเรื่องการให้ความยินยอมก็คือปัญหาเกี่ยวกับขนาดของหน้าจอโทรศัพท์เคลื่อนที่[87] ประเด็นก็คือผู้ให้บริการข้อมูลจะต้องให้ข้อมูลอะไรแก่ผู้ใช้บริการบ้างเพื่อให้พอดีและเหมาะกับพื้นที่ที่จำกัดของหน้าจอโทรศัพท์เคลื่อนที่

ดังนั้น ข้อมูลส่วนบุคคล (personal data) อันรวมถึงข้อมูลตำแหน่งของผู้ใช้บริการโทรศัพท์เคลื่อนที่ (location information for mobile users) ควรจะถูกจัดเก็บในสถานที่ที่เหมาะสมกับความรู้หรือความยินยอมของเจ้าของข้อมูลนั้นๆ การใช้ข้อมูลส่วนบุคคลใดใดก็ตามซึ่งอาจรวมถึงข้อมูลตำแหน่ง โดยที่ผู้บริโภคไม่ได้ให้ความตกลงไว้โดยชัดแจ้งสมควรที่จะถูกห้าม

---

[83] <www.soumu.go.jp/joho_tsusin/d_syohi/d_guide_01.html> (ภาษาญี่ปุ่น).

[84] อ้างถึง Ackerman *et al.,* 2003.

[85] <www.soumu.go.jp/joho_tsusin/d_syohi/pdf/051018_1.pdf> (ภาษาญี่ปุ่น).

[86] อ้างถึง OECD, 2005g.

[87] ดูหมวด "การเปิดเผยข้อมูลสำหรับหน้าจอขนาดเล็ก (Information disclosure for small screens)" ในส่วนที่ 3 (Part III) p. 24.

ในส่วนการให้ข้อมูลตำแหน่ง (location information) สามารถทำได้ในลักษณะที่เป็นบริการเสริม (value added services) เฉพาะเมื่อผู้ใช้บริการได้ให้ความยินยอมในเรื่องดังกล่าวอย่างเปิดเผย ภายใต้หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล และเพื่อที่จะได้รับความยินยอมจากผู้ใช้บริการ ผู้ให้บริการ (service provider) จะต้องแจ้งแก่สมาชิกว่าข้อมูลตำแหน่งประเภทไหนจะถูกนำมาใช้ เพื่อวัตถุประสงค์อะไร และใช้ช่วงเวลาใด และข้อมูลดังกล่าวจะถูกส่งไปยังบุคคลที่สามเพื่อวัตถุประสงค์ในการให้บริการอื่นอีกหรือไม่ ความยินยอมไม่สามารถถูกยกเป็นส่วนหนึ่งของข้อกำหนดและเงื่อนไขทั่วไปที่ถูกเสนอสำหรับการใช้บริการในการติดต่อสื่อสารทางระบบอิเล็กทรอนิกส์ (electronic communications) ได้ การได้รับการยินยอมอาจประกอบไปด้วยข้อตกลงที่มีเงื่อนไขให้แจ้งข้อมูลเต็มรูปแบบให้แก่ผู้ใช้บริการล่วงหน้าเกี่ยวกับกระบวนการระบุตำแหน่ง ทั้งนี้ ขึ้นอยู่กับชนิดของการให้บริการ นอกจากนี้ ผู้ให้บริการเสริมควรจะมีมาตรการที่เหมาะสม เพื่อให้แน่ใจว่าการยินยอมดังกล่าวถูกต้องตามกฎหมาย เมื่อขบวนการระบุตำแหน่งดำเนินไปอย่างต่อเนื่อง ผู้ให้บริการควรยืนยันการเป็นสมาชิกในการใช้บริการดังกล่าว โดยการส่งข้อความไปยังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการหลังจากที่ผู้ใช้บริการได้ให้ความยินยอมเป็นที่เรียบร้อยแล้ว และผู้รับบริการสามารถยกเลิกการยินยอมได้ทุกเมื่อที่ต้องการ ภายใต้หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล อีกทั้ง บุคคลที่ทำธุรกิจเกี่ยวกับระบบโทรคมนาคมไม่ควรเปิดเผยข้อมูลตำแหน่งแก่บุคคลอื่น ยกเว้นอยู่ภายใต้เงื่อนไขที่แน่นอน เช่น เมื่อเจ้าของข้อมูลนั้นได้ให้ความยินยอม นอกจากนี้ ในการปกป้องข้อมูลตำแหน่ง ผู้ให้บริการต้องส่งข้อความ เพื่อขอรับความยินยอมจากผู้รับบริการก่อนที่จะให้บริการต่างๆ และให้มีการยินยอมจากผู้รับบริการก่อนมีการจัดเก็บ การใช้ หรือการให้ข้อมูลตำแหน่ง อีกทั้ง วางบทลงโทษทางอาญา รวมถึงระยะเวลาการจำคุก สำหรับผู้ละเมิดกฎดังกล่าว

2.6.3 การเก็บรักษาและการโอนหรือส่งข้อมูลตำแหน่งไปให้แก่บุคคลที่สาม

มีหลายประเด็นที่เกี่ยวข้องกับคำถามที่ว่า ข้อมูลตำแหน่งประเภทไหนจะสามารถเก็บไว้ได้ได้บ้าง ผู้ให้บริการจะมีสิทธิเก็บข้อมูลไว้ได้นานแค่ไหน และเมื่อไหร่ข้อมูลดังกล่าวจะสามารถส่งไปยังบุคคลที่สามได้ ข้อมูลประเภทไหนที่จะถูกจัดเก็บนั้น มีความสำคัญมากเพราะจำนวนรายละเอียดอาจมีผลกระทบกับการใช้ข้อมูลในอนาคตที่อาจเกิดขึ้นได้ ข้อมูลจะถูกจัดเก็บได้นานแค่ไหนเป็นตัวกำหนดจำนวนครั้งการใช้ข้อมูลในอนาคต โดยเฉพาะอย่างยิ่ง ในเรื่องของการติดตามผลในระยะยาวและการจำแนกแบบแผน ยกตัวอย่างเช่น ถ้าข้อมูลตำแหน่งถูกบันทึกควบคู่ไปกับลำดับการดำเนินการที่น่าเชื่อถือ ข้อมูลข่าวสารจะสามารถเชื่อมต่อไปกับผู้ใช้บริการ

โดยตรงมากกว่าที่จะเชื่อมต่อผ่านโทรศัพท์เคลื่อนที่เพียงเท่านั้น การกำหนดในส่วนของความยินยอมจากผู้ใช้บริการจึงมีความสำคัญเป็นอย่างยิ่งเมื่อผู้ให้บริการเป็นผู้มีสิทธิส่งข้อมูลตำแหน่งของผู้ใช้บริการไปยังบุคคลที่สาม เพราะเป็นหน้าที่ของผู้ให้บริการที่ควรจะต้องเคารพความเป็นส่วนตัวในเรื่องข้อมูลข่าวสาร

ประเด็นที่เกิดขึ้นคือ ผู้ให้บริการหรือบุคคลที่สามอาจจะสามารถทราบข้อมูลของผู้ใช้บริการโดยการจับคู่ข้อมูลตำแหน่งกับฐานข้อมูลอื่นๆ จนอาจกลายเป็นการบุกรุกความเป็นส่วนตัวได้ เช่น บริษัทประกันภัยรถยนต์อาจคิดค่าเบี้ยประกันภัยมากขึ้นกับผู้ที่มักจะเดินทางเข้าไปในพื้นที่ที่มีความเสี่ยงบ่อยๆ กลุ่มเจรจาผู้บริโภคสองฟากฝั่งมหาสมุทรแอตแลนติก (TACD) ยังกล่าวเพิ่มเติมอีกว่า การสามารถเข้าไปดูข้อมูลผู้ใช้บริการได้อาจนำไปสู่แผนการตลาดที่ก่อให้เกิดการก้าวก่ายความเป็นส่วนตัวมากขึ้น[88]

ในสหภาพยุโรป หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล (Directive on Privacy and Electronic Communications) ได้มีการกำหนดถึงประเด็นนี้ไว้โดยเฉพาะ (EC มาตรา 29 Working Party, 2005) ว่าข้อมูลตำแหน่งอาจเพียงแค่ใช้ดำเนินการสำหรับ “ช่วงเวลาที่จำเป็นสำหรับการจัดเตรียมบริการเสริม” (Directive 2002/58/EC มาตรา 9(1)) ตามที่ EC มาตรา 29 ว่าด้วยการประสานความร่วมมือกันระหว่างหน่วยงานด้านการคุ้มครองข้อมูล (Data Protection Working Party (2005)) ได้ระบุไว้มีข้อสังเกตว่า ผู้ให้บริการไม่สิทธิที่จะเก็บข้อมูลตำแหน่งของผู้ใช้บริการซึ่งเคยนำมาใช้ในการให้บริการแล้วครั้งหนึ่งไว้ แต่ถ้าหากผู้ให้บริการต้องการเก็บบันทึกข้อมูลตำแหน่งของผู้ใช้บริการไว้ ก็จะต้องทำให้ข้อมูลดังกล่าวเป็นข้อมูลที่ไม่มีการระบุชื่อ หรือข้อมูลนิรนามเสียก่อน (data anonymous)[89]

---

[88] อ้างถึง TACD, 2005.

[89] เพื่อที่จะคงความไม่มีลักษณะเฉพาะ (anonymity) หรืออนุญาตให้ผู้ใช้ควบคุมข้อมูลบนพื้นฐานความพึงพอใจของแนวนโยบายความเป็นส่วนตัว ผู้เชี่ยวชาญได้เสนอระบบสถาปัตยกรรมใหม่เพื่อพัฒนาการคุ้มครองความเป็นส่วนตัวของข้อมูลตำแหน่ง ตัวอย่างเช่น Nakanishi et al. (2004) ได้เสนอว่า เครื่องตรวจจับลักษณะเฉพาะ (identity detectors) ควรจะแยกออกจากโปรมแกรมที่ทำให้ทราบตำแหน่ง (location-aware applications) Ahmad et al. (2004) ได้เสนอว่าให้นำรายการควบคุมการเข้าถึง (an access control list) และเครื่องคอมพิวเตอร์แม่ข่ายควบคุมการเข้าถึง (access management severs) มาใช้กับข้อมูลตำแหน่งทางภูมิศาสตร์ (geographic location information) Gakparia et al. (2004) ได้เสนอว่า

อย่างไรก็ตาม ประเทศฟินแลนด์ได้ให้ข้อสังเกตว่าข้อมูลที่ไม่สามารถระบุที่มาที่ไปได้และไม่สามารถเชื่อมต่อกับบุคคลใดบุคคลหนึ่งได้โดยเฉพาะอาจจะสามารถใช้ได้อย่างอิสระ ปัญหาของการแปลความเกี่ยวเนื่องกับคำถามที่ว่า แล้วเมื่อไหร่ถึงจะเป็นข้อมูลไม่สามารถระบุที่มาที่ไปและไม่เชื่อมต่อกับบุคคลใดได้อย่างแท้จริง และเมื่อไหร่ที่จะเป็นข้อมูลที่มีความชัดเจนว่าเกี่ยวข้องกับสมาชิกหรือผู้ใช้บริการ สถานการณ์ดังที่กล่าวมาอาจเกิดขึ้นได้ ยกตัวอย่างเช่น เมื่อมีจำนวนประชากรไม่มากในบริเวณหนึ่งๆหรือด้วยพื้นที่ที่จำกัด จึงทำให้สามารถทำนายความเคลื่อนไหวได้ล่วงหน้าว่าจะเกิดอะไรขึ้นต่อไป แม้ข้อมูลดังกล่าวอาจยังไม่เชื่อมต่อกับบุคคลใดก็ตาม บริษัทที่ดำเนินกิจการเกี่ยวกับโทรคมนาคมและผู้ให้บริการโทรศัพท์เคลื่อนที่ซึ่งมีหน้าที่จัดการข้อมูลดังกล่าว จะเป็นผู้ดำเนินการข้อมูลตำแหน่งเหล่านี้ แต่อย่างไรก็ตาม ประเทศฟินแลนด์ก็ให้เหตุผลว่าอาจมีความเสี่ยงเกิดขึ้นหากข้อมูลตำแหน่งนั้นถูกประมวลผลโดยบุคคลที่ไม่มีสิทธิในการดำเนินงาน หรือข้อมูลนั้นได้รับการช่วยเหลือจากเทคโนโลยีเพื่อวัตถุประสงค์ ที่อาจก่อให้เกิดการละเมิดความเป็นส่วนตัวได้[90]

ภายใต้หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล (มาตรา 9 (1) แห่ง Directive 2002/58/EC) ผู้ให้บริการจะต้องแจ้งผู้ใช้บริการก่อนที่จะขอรับความยินยอมจากผู้ใช้บริการถึงประเภทของที่ตั้งข้อมูลที่จะใช้ดำเนินการ อีกทั้ง ยังรวมถึงการยอมรับวัตถุประสงค์ หรือระยะเวลาของการประมวลผล รวมถึงการที่ข้อมูลดังกล่าวอาจถูกส่งไปยังบุคคลที่สามเพื่อวัตถุประสงค์ในการให้บริการที่เพิ่มมูลค่าขึ้นไปอีก และยังเพิ่มเติมอีกว่าข้อมูลจะต้องไม่ถูกส่งยังบุคคลที่สามยกเว้นเพื่อวัตถุประสงค์ดังที่กล่าวมาเท่านั้น (มาตรา 9(3))

ในขณะที่คณะกรรมการกลางกำกับดูแลกิจการสื่อสารของสหรัฐเมริกา (Federal Communications Commission: FCC) เลือกใช้วิธีที่ตรงข้ามกับทางสหภาพยุโรป คือ ไม่ออกกฎเกี่ยวกับข้อปฏิบัติในเรื่องข้อมูลตำแหน่ง โดยให้เหตุผลว่าการให้บริการข้อมูลตำแหน่ง (location-based services) เพิ่งเกิดขึ้นไม่นาน และทางคณะกรรมการกลางกำกับดูแลกิจการสื่อสารของสหรัฐเมริกา (Federal Communications Commission: FCC) เองก็ไม่ปรารถนาที่จะบังคับตัวเทคโนโลยี หรือทางเลือกของผู้บริโภคโดยการใช้กฎ[91] อย่างไรก็ตาม ในสหรัฐฯเองก็มีความพยายามที่จะใช้การกำกับดูแลตนเอง ตัวอย่างเช่น สมาคมการตลาดผ่านโทรศัพท์เคลื่อนที่

บุคคลภายนอกที่เชื่อถือได้ (trusted third party) ควรจะเป็นผู้มีส่วนเกี่ยวข้องในการควบคุมความเป็นส่วนตัวของข้อมูลตำแหน่ง (location information).

[90] อ้างถึง OECD, 2004c.

[91] อ้างถึง FCC, 2002.

(Mobile Marketing Association) และ สมาคมการสื่อสารและอินเตอร์เน็ต (Cellular Telecommunications and Internet Association) ได้กำหนดแนวทางเกี่ยวกับการคุ้มครองข้อมูลตำแหน่งขึ้นมา[92]

ในทางธุรกิจ ผู้ให้บริการหลายรายได้นำประเด็นนี้มาไว้ในนโยบายความเป็นส่วนตัวหรือนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy policy) ของพวกเขาด้วย ตัวอย่างเช่น O2 ผู้ให้บริการระบบปฏิบัติการโทรศัพท์เคลื่อนที่ในประเทศอังกฤษ ได้จัดให้มีการควบคุมความเป็นส่วนตัวจากบริการข้อมูลตำแหน่ง (Location Services Privacy Controller: LSPC) ซึ่งบริการนี้ผู้บริโภคสามารถปฏิเสธที่จะเปิดเผยข้อมูลตำแหน่งในบางบริการหรือทั้งหมดก็ได้

ในขณะที่แต่ละประเทศเลือกใช้วิธีที่แตกต่างกัน แต่จะเห็นได้ว่าทุกวิธีก็มีใจความหลักไปในทางเดียวกัน คือ การได้รับความยินยอมอย่างชัดแจ้งในเรื่องการเก็บรวบรวมข้อมูลและการใช้ข้อมูลตำแหน่งของแต่ละบุคคลเป็นปัจจัยที่สำคัญต่อการคุ้มครองความเป็นส่วนตัว ซึ่งใจความดังกล่าวก็สอดคล้องกับแนวทางเรื่องความเป็นส่วนตัวขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Privacy Guidelines)

ดังนั้น ข้อมูลตำแหน่งอาจเพียงแค่ใช้ดำเนินการสำหรับช่วงเวลาที่จำเป็นสำหรับการจัดเตรียมบริการเสริม ผู้ให้บริการไม่สิทธิที่จะเก็บข้อมูลตำแหน่งของผู้ใช้บริการซึ่งเคยนำมาใช้ในการให้บริการแล้วครั้งหนึ่งไว้ แต่ถ้าหากผู้ให้บริการต้องการเก็บบันทึกข้อมูลตำแหน่งของผู้ใช้บริการไว้ ก็จะต้องทำให้ข้อมูลดังกล่าวเป็นข้อมูลที่ไม่มีการระบุชื่อ หรือข้อมูลนิรนามเสียก่อน (data anonymous) เนื่องจากข้อมูลที่ไม่สามารถระบุที่มาที่ไปได้และไม่สามารถเชื่อมต่อกับบุคคลใดบุคคลหนึ่งได้โดยเฉพาะอาจจะสามารถใช้ได้อย่างอิสระ แม้ข้อมูลดังกล่าวอาจยังไม่เชื่อมต่อกับบุคคลใดก็ตาม บริษัทที่ดำเนินกิจการเกี่ยวกับโทรคมนาคมและผู้ให้บริการโทรศัพท์เคลื่อนที่ซึ่งมีหน้าที่จัดการข้อมูลดังกล่าว จะเป็นผู้ดำเนินการข้อมูลตำแหน่งเหล่านี้ แต่อย่างไรก็ตาม อาจมี

---

[92] สมาคมการตลาดผ่านโทรศัพท์เคลื่อนที่ (Mobile Marketing Association: MMA) และ สมาคมการสื่อสารระบบเซลลูลาร์และอินเตอร์เน็ต (Cellular Telecommunications and Internet Association: CTIA) ได้พัฒนา"คู่มือแนวปฏิบัติอันเป็นเลิศสำหรับการให้บริการข้อมูลผ่านอุปกรณ์สื่อสารเคลื่อนที่" (Best Practices Guidelines for Cross-Carrier Mobile Content Services) ตาม <www.mmaglobal.com/bestpractices.pdf> และสมาคมการสื่อสารระบบเซลลูลาร์และอินเตอร์เน็ต (Cellular Telecommunications and Internet Association: CTIA) ยังมีคู่มือของตนเองคือ “ประมวลกฎหมายคุ้มครองผู้บริโภคสำหรับบริการไร้สาย” (Consumer Code for Wireless Service) ตาม <files.ctia.org/pdf/The_Code.pdf>.

ความเสี่ยงเกิดขึ้น หากข้อมูลตำแหน่งนั้นถูกประมวลผลโดยบุคคลที่ไม่มีสิทธิในการดำเนินงาน หรือข้อมูลนั้นได้รับการช่วยเหลือจากเทคโนโลยี เพื่อวัตถุประสงค์ที่อาจก่อให้เกิดการละเมิดความเป็นส่วนตัวได้ ผู้ให้บริการจะต้องแจ้งผู้ใช้บริการก่อนที่จะขอรับความยินยอมจากผู้ใช้บริการ ถึงประเภทของที่ตั้งข้อมูลที่จะใช้ดำเนินการ อีกทั้ง การยอมรับวัตถุประสงค์ หรือระยะเวลาของการประมวลผล รวมถึงการที่ข้อมูลดังกล่าวอาจถูกส่งไปยังบุคคลที่สามเพื่อวัตถุประสงค์ในการให้บริการเสริมอื่น ที่สำคัญข้อมูลจะต้องไม่ถูกส่งยังบุคคลที่สาม ยกเว้นเพื่อวัตถุประสงค์ดังที่กล่าวมาเท่านั้น ในการควบคุมความเป็นส่วนตัวจากบริการข้อมูลตำแหน่ง (Location Services Privacy Controller: LSPC) ผู้บริโภคสามารถปฏิเสธที่จะเปิดเผยข้อมูลตำแหน่งในบางบริการหรือทั้งหมดก็ได้

2.7 ประเด็นความปลอดภัย

แม้ว่าประเด็นเรื่องความเป็นส่วนตัวเป็นประเด็นที่ได้รับความสนใจเป็นอย่างมาก แต่ประเด็นเรื่องความปลอดภัยก็ยังถูกกำหนดให้มีความสำคัญในการพาณิชย์ทางโทรศัพท์เคลื่อนที่ (mobile commerce) ด้วยเช่นกัน แต่อาจมีเฉพาะในกรณีที่โทรศัพท์เคลื่อนที่นั้นมีระบบ Infrared ติดตั้งในตัวเครื่อง เช่น IrDA หรือ โทรศัพท์เคลื่อนที่ที่มีเทคโนโลยีความถี่วิทยุในตัว (radio frequency technology) เช่น Bluetooth, RFID tag และ Contactless card หรือเทคโนโลยีที่ใกล้เคียง ซึ่งได้นำมาใช้เป็นวิธีการชำระค่าบริการแล้วในบางประเทศ[93] ในส่วนที่จะกล่าวถัดไปจะ

---

[93] ดู DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY COMMITTEE ON CONSUMER POLICY, MOBILE COMMERCE (DSTI/CP(2006)7/FINAL), 16-Jan-2007, Part II เรื่องการพัฒนาทางเทคโนโลยี ซึ่ง Contactless card หรือเทคโนโลยีที่ใกล้เคียงถูกใช้สำหรับบริการผสมผสานทางการเงินทางโทรศัพท์เคลื่อนที่ (integrated mobile financial services) ดังนั้น ระบบรักษาความปลอดภัยของ Contactless card คือประเด็นสำคัญเมื่อประเด็นการรักษาความปลอดภัยในการชำระเงิน (payment security issues) ถูกนำมาถกเถียงกัน ถึงแม้ว่า ประเด็นระบบรักษาความปลอดภัยของ Contactless card ดังกล่าวจะมิได้มีการกล่าวไว้ในรายงานนี้ (DSTI/CP(2006)7/FINAL) ก็ตาม, โปรดดู ภาคผนวก ข.

มุ่งเน้นไปที่เทคโนโลยีบลูทูธ (Bluetooth technology)[94] ยิ่งไปกว่านั้น ความเป็นไปได้ที่ไวรัส (viruses) และหนอนอินเตอร์เน็ต (worms) ซึ่งอาจก่อให้เกิดผลกระทบในวงกว้างต่อโทรศัพท์เคลื่อนที่ในอนาคตนั้น อาจกลายมาเป็นสิ่งที่ต้องให้ความสำคัญด้วย

2.7.1 ประเด็นความปลอดภัยอันเกิดจากเทคโนโลยี Bluetooth

เทคโนโลยี Bluetooth ถูกประยุกต์ใช้ในโทรศัพท์เคลื่อนที่เพิ่มมากขึ้น Bluetooth เป็นเทคโนโลยีที่ใช้คลื่นความถี่วิทยุ (radio frequency waves) เป็นตัวสื่อสารแบบไร้สาย (communicate wirelessly) ระหว่าง Bluetooth และอุปกรณ์ที่รองรับได้ (enabled devices) ตัวอย่างเช่น ผู้ใช้บริการอาจส่งบัตรเชิญทางธุรกิจไปยังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการอื่น หรือใช้หูฟังแบบไร้สายเพื่อพูดทางโทรศัพท์เคลื่อนที่ ในสหรัฐอเมริกา 11% ของผู้บริโภคมีเทคโนโลยีนี้ในโทรศัพท์เคลื่อนที่ของตน และ 45% ของผู้บริโภคที่มีเทคโนโลยีนี้ได้มีการใช้งานมัน[95] และมากกว่า 30% ของผู้บริโภคคาดหวังที่จะมีเทคโนโลยีเหล่านี้ไว้ในครอบครอง

รูปแบบความปลอดภัยสำหรับโทรศัพท์เคลื่อนที่ที่สามารถใช้บริการ Bluetooth ได้คือ มันจะไม่สามารถสื่อสารได้ จนกว่าจะเกิดการจับคู่กันโดยการได้รับอนุญาตเกิดขึ้น (paired) นี่เป็นขบวนการซึ่งอุปกรณ์ทั้งสองจะต้องใส่หมายเลขรหัสบุคคล (PIN number) ที่เหมือนกันลงไป ดังนั้นขบวนการดังกล่าวจึงสามารถจำกัดความเป็นไปได้ในการก่อให้เกิดความไม่ปลอดภัยได้เนื่องจากต้องใช้ระยะทางที่สั้นในการดำเนินขบวนการดังกล่าว (โดยทั่วไปคือระยะประมาณ 10 เมตรจากโทรศัพท์เคลื่อนที่)[96]

ผู้เจาะระบบข้อมูลหลายคน (Hackers) ได้พยายามล้วงข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่ผ่านเทคโนโลยี Bluetooth ความสามารถของผู้เจาะระบบข้อมูล (Hackers) ในการเข้าถึงข้อมูลที่อยู่ในโทรศัพท์เคลื่อนที่ของผู้ใช้บริการ ก่อให้เกิดประเด็นทั้งทางด้านความเป็นส่วนตัว และความปลอดภัยขึ้น การลักลอบส่งข้อความผ่านโทรศัพท์เคลื่อนที่ของผู้อื่นโดยใช้ระบบเน็ตเวิร์ค Bluetooth (Bluejacking) เป็นตัวอย่างหนึ่งในการใช้เทคโนโลยี Bluetooth ไปในทางที่ไม่

---

[94] การเจาะ (Hacking) เข้าไปในเทคโนโลยีอื่นๆก็สามารถเกิดขึ้นได้ เช่น side channel attack และ crypt-analysis ตามตัวอย่างใน Witteman (2006) Handschuh (2004) <http://cq.cx/proxmark3.pl>.

[95] อ้างถึง Rockbridge Associates and Robert H. Smith School of Business, University of Maryland, 2006.

[96] อ้างถึง Whitehouse, 2003.

เหมาะสม เพราะ Bluetooth อนุญาตให้ผู้ใช้บริการโทรศัพท์เคลื่อนที่ส่งนามบัตรนิรนามไปยังโทรศัพท์เคลื่อนที่ของผู้อื่น การลักลอบส่งข้อความผ่านโทรศัพท์เคลื่อนที่ของผู้อื่นโดยใช้ระบบเน็ตเวิร์ค Bluetooth (Bluejacking) ไม่ได้ก่อให้เกิดการคุกคามด้านระบบความปลอดภัยของผู้รับนามบัตรนั้น เนื่องจากข้อมูลที่ถูกส่งไปจะไม่สามารถเคลื่อนย้ายหรือปรับเปลี่ยนได้ แต่อย่างไรก็ตาม การลักลอบส่งข้อความผ่านโทรศัพท์เคลื่อนที่ของผู้อื่นโดยใช้ระบบเน็ตเวิร์ค Bluetooth (Bluejacking) ถือเป็นการล่วงละเมิดชนิดหนึ่ง โดยเฉพาะถ้าการส่งข้อความนั้นเต็มไปด้วยข้อความที่มีลักษณะเป็นการหมิ่นประมาทหรือข่มขู่ (abusive หรือ threatening language)[97]

การเจาะโทรศัพท์เคลื่อนที่ผ่านทาง Bluetooth (Bluesnarfing) มักจะใช้เพื่อการขโมยข้อมูล เช่น เบอร์โทรศัพท์ ข้อมูลในปฏิทินบนโทรศัพท์เคลื่อนที่[98] ผู้เจาะระบบข้อมูล (Hackers) จะดำเนินการโดยอยู่ห่างจากโทรศัพท์เคลื่อนที่ที่ต้องการจะเจาะข้อมูลไม่เกิน 10 เมตร โดยใช้ซอฟแวร์แบบพิเศษ แต่มีเพียงโทรศัพท์เคลื่อนที่ที่สามารถใช้ระบบ Bluetooth รุ่นเก่าๆ เท่านั้นที่ง่ายต่อการถูก Bluesnarfing อย่างไรก็ตาม ถ้าโทรศัพท์เคลื่อนที่เหล่านี้ถูกตั้งให้อยู่ในระบบที่ “ไม่สามารถถูกค้นพบได้” (non-discoverable) ก็จะยากต่อผู้เจาะระบบข้อมูล (Hackers) ในการเข้าไปขโมยข้อมูลของผู้ใช้โทรศัพท์เคลื่อนที่นั้นๆ ดังนั้นประเด็นในเรื่องความปลอดภัยส่วนใหญ่ที่เกิดขึ้นโดย Bluesnarfing จึงสามารถจัดการได้[99]

จุดอ่อนอื่นๆของระบบ Bluetooth คือ มีความเป็นไปได้ที่ผู้เจาะระบบข้อมูล (Hackers) จะสามารถถอดรหัสเข้าไปในอุปกรณ์ที่สามารถใช้ระบบ Bluetooth จากนั้นก็ควบคุมอุปกรณ์นั้นไว้[100] แม้ว่าการกระทำนี้จะถูกจำกัดเพราะโทรศัพท์เคลื่อนที่นั้นใช้ระบบทำตามคำสั่งของผู้ใช้โทรศัพท์นั้นๆ (custom Bluetooth device)[101] และจะไม่สามารถเจาะเข้าระบบได้โดยใช้อุปกรณ์ที่มีทั่วไปตามท้องตลาด อย่างไรก็ตาม ผู้ใช้โทรศัพท์เคลื่อนที่เองก็ต้องระวังความเสี่ยงที่

---

[97] Bluejack Q, “What is Bluejacking?” ดู: <www.bluejackq.com>.

[98] อ้างถึง Laurie *et al.,* 2004.

[99] อีกเทคนิค คือ “Bluebugging” ที่สามารถจะเข้าถึงโทรศัพท์เคลื่อนที่ด้วยบลูทูธ (Bluetooth technology) โดยเจ้าของไม่รู้ตัว และใช้โทรศัพท์หรือฟังการสนทนาทางโทรศัพท์ผ่านเครื่องที่ถูกโจมตีได้ อย่างไรก็ตาม มีเพียงBluetooth ไม่กี่แบบเท่านั้นที่ง่ายต่อการถูก Bluebugging และบริษัทผู้ผลิตได้ทำการแก้ไขปัญหาแล้ว ดูข้อมูลเพิ่มเติมที่เว็บไซต์ของ Bluetooth Special Interest Group ใน <www.bluetooth.com/Bluetooth/Learn/Security/>.

[100] อ้างถึง Shaked and Wool, 2005.

[101] <www.bluejackq.com>.

อาจเกิดขึ้นเหล่านี้ และอาจป้องกันตัวเองได้โดยเปลี่ยนมาใช้รหัสบุคคล (PIN) จากสี่หลักมาเป็นแปดหลักเพื่อลดความเสี่ยงจากการถูกถอดรหัสโดยผู้เจาะระบบข้อมูล (Hackers)

สิ่งที่เน้นมากในหลักการข้อที่ 1 ของ แนวการปฏิบัติสำหรับการรักษาปลอดภัยของเครือข่ายและระบบข้อมูล โดยองค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines for the Security of Information Systems and Networks) คือ การป้องกันเบื้องต้นเกี่ยวกับปัญหาเรื่องความปลอดภัยคือ ระวังกับความเสี่ยงที่อาจเกิดขึ้นและเตรียมพร้อมสำหรับการป้องกันปัญหาเสมอ เพราะพนักงานส่วนใหญ่มักจะเก็บข้อมูลความลับทางธุรกิจ ไม่ว่าจะเป็นรายชื่อ จดหมายอิเล็กทรอนิกส์ (E-mail) และรหัสผ่าน (Password) ไว้บนโทรศัพท์เคลื่อนที่ของตนเสมอ ดังนั้น นายจ้างควรจะทำให้แน่ใจว่าลูกจ้างของตนให้ความระมัดระวังในเบื้องต้นเพื่อเป็นการยกระดับความปลอดภัยได้ดีเพียงใด ตัวอย่างเช่น สถาบันมาตรวิทยาของสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ได้สร้างแนวทางการตรวจสอบความปลอดภัยจากการใช้ระบบ Bluetooth เพื่อรักษาความปลอดภัยของระบบดังกล่าว[102] นอกจากนี้ United States computer Emergency Readiness Team (US-CERT)[103] และBluetooth Special Interest Group[104] ได้สร้างแนวทางสำหรับผู้ใช้บริการโทรศัพท์เคลื่อนที่ว่าทำอย่างไรจึงสามารถสร้างการป้องกันความปลอดภัยจากการบุกรุกผ่านโทรศัพท์เคลื่อนที่ได้เช่นกัน

ข้อแนะนำโดยทั่วไปก็คือ ปิดระบบ Bluetooth เมื่อไม่ต้องการใช้ และตรวจสอบว่าระบบอยู่ในโหมด “ไม่สามารถถูกค้นพบ” เมื่อต้องการใช้ระบบดังกล่าว ทั้งนี้ ผู้ใช้บริการระบบเคลื่อนที่เองก็ต้องระมัดระวัง และสังเกตสภาพแวดล้อมขณะใช้งาน Bluetooth ด้วย ความเสี่ยงอาจเกิดมากขึ้นได้หากเกิดการติดต่อโดยใช้ระบบ Bluetooth ผ่านบริการอินเตอร์เน็ตสาธารณะโดยเครือข่ายไร้สาย ดังนั้น ผู้ใช้บริการจึงควรได้รับการแนะนำเกี่ยวกับวิธีการปฏิบัติเมื่อใช้บริการดังกล่าว ทั้งนี้ ผู้ใช้บริการควรใช้รหัสบุคคล (PIN) อย่างน้อย 8 หลัก และควรแชร์ข้อมูลกับบุคคลที่ไว้ใจได้เท่านั้น ดังนั้น ผู้ใช้ระบบ Bluetooth ทั้งหลาย ควรระวังความเสี่ยงและหาทางป้องกันเพื่อก่อให้เกิดความปลอดภัยไว้แต่แรกๆ

ผู้ผลิตโทรศัพท์เคลื่อนที่ที่มีเทคโนโลยี Bluetooth อยู่ภายใน จะต้องเริ่มแก้ปัญหาในเรื่องความเสี่ยงต่อระบบความปลอดภัย และตอบสนองต่อรูปแบบการจัดการกับปัญหาที่เกิดขึ้นอย่างเหมาะสมและทันท่วงที (ตามหลักการข้อที่ 3 ของแนวทางเพื่อความปลอดภัยขององค์การ

---

[102] อ้างถึง Karygiannis and Owens, 2002.

[103] McDowell, M., Lytle, M. (2005) “Understanding Bluetooth Technology”.

[104] อ้างถึง Bluetooth SIG, 2006a.

เพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Security Guidelines)) ผู้ผลิตจะต้องแจ้งข้อเสียของเทคโนโลยี Bluetooth ที่สามารถเกิดขึ้นได้แน่นอน และพัฒนาระบบซอร์ฟแวร์เพื่อช่วยแก้ปัญหาดังกล่าวด้วย[105] ดังนั้นผู้ผลิตโทรศัพท์เคลื่อนที่ควรจะประเมินค่าความเสี่ยงเพื่อบอกถึงการคุกคามและข้อด้อยในเทคโนโลยี Bluetooth และหามาตรการการป้องกันอันอาจเกิดจากเหตุดังกล่าว (ตามหลักการข้อที่ 6 ของแนวทางเพื่อความปลอดภัยขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Security Guidelines))

ดังนั้น ในประเด็นความปลอดภัยอันเกิดจากเทคโนโลยี Bluetooth เนื่องจาก Bluetooth จะไม่สามารถสื่อสารได้ จนกว่าจะเกิดการจับคู่กันโดยการได้รับอนุญาตเกิดขึ้น (paired) โดยอุปกรณ์ทั้งสองจะต้องใส่หมายเลขรหัสบุคคล (PIN number) ที่เหมือนกันลงไป ดังนั้น กระบวนการดังกล่าวจึงสามารถจำกัดความเป็นไปได้ในการก่อให้เกิดความไม่ปลอดภัยได้ เนื่องจากต้องใช้ระยะทางที่จำกัดในการดำเนินขบวนการดังกล่าว และผู้ใช้โทรศัพท์เคลื่อนที่อาจป้องกันตัวเองได้ โดยเปลี่ยนมาใช้รหัสบุคคล (PIN) จาก 4 หลักมาเป็น 8 หลักเพื่อลดความเสี่ยงจากการถูกถอดรหัสโดยผู้เจาะระบบข้อมูล (Hackers) และควรแชร์ข้อมูลกับบุคคลที่ไว้ใจได้เท่านั้น ทั้งต้องระมัดระวังและสังเกตสภาพแวดล้อมขณะใช้งาน Bluetooth ด้วย ข้อแนะนำโดยทั่วไปก็คือ ควรปิดระบบ Bluetooth ทุกครั้งเมื่อไม่ต้องการใช้ และตรวจสอบว่าระบบอยู่ในโหมดที่ไม่สามารถถูกค้นพบ เมื่อต้องการใช้ระบบดังกล่าว แต่ก็อาจเกิดความเสี่ยงมากขึ้นได้ หากเกิดการติดต่อโดยใช้ระบบ Bluetooth ผ่านบริการอินเตอร์เน็ตสาธารณะโดยเครือข่ายไร้สาย ดังนั้น ผู้ใช้บริการจึงควรได้รับการแนะนำเกี่ยวกับวิธีการปฏิบัติเมื่อใช้บริการดังกล่าว นอกจากนี้ ผู้ผลิตจะต้องแจ้งข้อเสียของเทคโนโลยี Bluetooth ที่สามารถเกิดขึ้นได้แน่นอน และพัฒนาระบบซอร์ฟแวร์เพื่อช่วยแก้ปัญหาดังกล่าวด้วย

2.7.2 **ความเสี่ยงอันเกิดจากไวรัส** (Viruses) **และหนอนอินเตอร์เน็ต** (Worms)

ประเด็นที่เกี่ยวกับการคุกคามระบบการรักษาความปลอดภัย (Security threat) บนโทรศัพท์เคลื่อนที่อันเกิดจากไวรัสได้เพิ่มมากขึ้น[106] แม้จะมีบางคนตั้งคำถามว่าการคุกคามของไวรัสบนโทรศัพท์เคลื่อนที่เป็นเรื่องอันตรายอย่างไร[107] ความจริงที่ว่า ปัจจุบันข้อมูลสำคัญทางการเงิน (financial data) หรือข้อมูลอัตราแลกเปลี่ยน (exchange information) ที่บรรดาอาชญา

---

[105] อ้างถึง Bluetooth SIG, 2006b.

[106] อ้างถึง IBM, 2005.

[107] อ้างถึง IBM, 2006.

กร (criminals) ทั้งหลายต้องการมันจะถูกจัดเก็บบนโทรศัพท์เคลื่อนที่ ดังนั้น ประเด็นเรื่องไวรัสบนโทรศัพท์เคลื่อนที่จึงกลายเป็นประเด็นที่ต้องถกเถียงกันในปัจจุบัน

รายงาน ณ ปัจจุบันแสดงให้เห็นว่าการติดไวรัสบนโทรศัพท์เคลื่อนที่นั้นยังมีอัตราที่ต่ำ ทั้งนี้ อาจเป็นเพราะอัตราการใช้อินเตอร์เน็ต (internet) บนโทรศัพท์เคลื่อนที่ยังมีไม่มากนั่นเอง โดยเฉพาะก่อนที่จะมีโทรศัพท์เคลื่อนที่แบบ 3G[108] ออกมาในตลาด รวมถึงความหลากหลายของระบบปฏิบัติการที่ผู้ผลิตเลือกใช้อาจทำให้ไวรัสแพร่กระจายได้ยากขึ้น[109] นักวิเคราะห์บางคนพิจารณาว่า ไวรัสและหนอนอินเตอร์เน็ตไม่สามารถแพร่กระจายไปยังโทรศัพท์เคลื่อนที่จำนวนมากได้ เพราะโทรศัพท์ที่สามารถใช้บริการทางอินเตอร์เน็ตได้ (Internet-connectable phones) และผู้ใช้บริการมีการใช้บริการอย่างสม่ำเสมอมีเพียง 30% ของโทรศัพท์เคลื่อนที่ทั้งหมด ทั้งนี้ ไม่อาจจะคาดเดาว่าจะเกิดขึ้นจนกว่าจะถึงสิ้นปี 2007[110]

อย่างไรก็ตาม แม้อัตราความเสี่ยง ณ ปัจจุบันยังต่ำอยู่ แต่จำนวนเป้าหมายของไวรัสบนโทรศัพท์เคลื่อนที่ก็เพิ่มสูงขึ้น ตัวอย่างเช่น รายงานของ Trend Micro กล่าวว่า พบไวรัส 140 ตัวบนโทรศัพท์เคลื่อนที่นับจนถึงเดือนมีนาคม 2006 (เช่น Cabir, QDial, RedBrowser และ Mabir)[111] บริษัท F-Secure ผู้ผลิตโปรแกรมต่อต้านไวรัสรายงานว่าปัจจุบันพบไวรัสอยู่บนโทรศัพท์เคลื่อนที่ (mobile viruses) กว่า 200 ตัวเคลื่อนไหวโดยอิสระอยู่[112] ไวรัสบนโทรศัพท์สามารถแพร่กระจายไปได้หลายทาง เช่น ผ่านทางเว็บไซต์ที่ไม่ประสงค์ดี (malicious websites) การแนบมากับไปรษณีย์อิเล็กทรอนิกส์ (e-mail attachments) การใช้เทคโนโลยี Bluetooth และการใช้บริการข้อความสั้น (SMS text messages)

ตัวอย่างเช่น ปัจจุบันมีม้าโทรจัน (Trojan horse) ชนิดหนึ่งชื่อ Red Browser เป็นแอพพลิเคชันที่ดูเหมือนใช้สำหรับเข้าสู่ WAP pages โดยผ่านข้อความสั้น (SMS) ไปรษณีย์อิเล็กทรอนิกส์ (E-mail) ที่ไม่เสียค่าใช้จ่าย ในขณะที่แท้จริงแล้วจะส่งข้อความผ่านข้อความสั้น (SMS) ไปยังหมายเลขที่ต้องเสียค่าใช้จ่ายในอัตราที่สูงมาก หนอนไวรัสพวก Mabir,

---

[108] 3G หรือ Third Generation: อุปกรณ์ที่ผสมผสาน การนำเสนอข้อมูล และเทคโนโลยีในปัจจุบันเข้าด้วยกัน

[109] อ้างถึง Cousins, 2005.

[110] อ้างถึง Pescatore and Girard, 2005.

[111] ดู Trend Micro (2005) เกี่ยวกับความเป็นมาและลักษณะของไวรัสต่างๆบนโทรศัพท์เคลื่อนที่.

[112] อ้างถึง F-Secure, 2006.

Commwarrior และ ไวรัสตัวอื่น ใช้ข้อความมัลติมีเดีย (MMS) และสามารถแพร่กระจายตัวเองผ่านทางเครือข่ายโทรศัพท์เคลื่อนที่ (mobile networks) ได้ เมื่อเปรียบเทียบกับไวรัสที่สามารถแพร่กระจายผ่านระบบ Bluetooth โอกาสในการแพร่กระจายของไวรัสจะเพิ่มมากขึ้น ไวรัสส่วนมากในปัจจุบันจะแพร่กระจายไปยังโทรศัพท์เครื่องที่ที่ใช้ระบบปฏิบัติการที่ออกแบบมาเพื่อรองรับเทคโนโลยีการสื่อสารแบบไร้สาย (Wireless) ที่ช่วยในการส่งข้อมูลของโทรศัพท์เคลื่อนที่เป็นหลัก (Symbian OS-based operating system)

นอกจากนี้ ผู้ใช้บริการจะต้องยอมรับข้อความที่มีไวรัส ก่อนที่ไวรัสเหล่านี้จะแพร่ไปยังตัวโทรศัพท์ อย่างไรก็ตาม ตามที่ได้วิเคราะห์กันไว้ สาเหตุหลักเป็นเพราะเจ้าของโทรศัพท์เคลื่อนที่ขาดความรู้ความเข้าใจเกี่ยวกับการคุกคามของไวรัสทางโทรศัพท์เคลื่อนที่เหล่านี้ ดังนั้น จึงมีโอกาสเป็นไปได้สูงที่จะเปิดข้อความที่ส่งมาโดยไปรษณีย์อิเล็กทรอนิกส์ (e-mail) จากเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ที่มีธงแดง (Red Flags) อยู่ นักวิเคราะห์เชื่อว่าอีกไม่นานผู้ที่เขียนโปรแกรมไวรัสสำหรับโทรศัพท์เคลื่อนที่ จะหาทางพัฒนาโปรแกรมไวรัสที่สามารถสร้างผลประโยชน์จากการเข้าไปขโมยข้อมูล (hacking) มากขึ้น[113]

คำถามที่ว่า แล้วผู้ผลิต (manufacturers) และผู้ใช้โทรศัพท์เคลื่อนที่จะป้องกันการแพร่กระจายของไวรัสบนโทรศัพท์เคลื่อนที่ (mobile viruses) ได้อย่างไรนั้น ผู้ดำเนินธุรกิจโทรศัพท์เคลื่อน (mobile phone operators) บางรายเริ่มที่จะพุ่งเป้าไปที่ระบบเครือข่าย (network) ตรวจรายละเอียดข้อความ เพื่อที่จะกลั่นกรองโปรแกรมที่ก่อให้เกิดความเสียหาย (Evers, n.d.) อุปกรณ์โทรศัพท์เคลื่อนที่ปัจจุบันบางรุ่น เช่น Nokia 6670 Nokia 9500 และ NTT DoCoMo 901i ได้มีการลงโปรแกรมป้องกันไวรัสก่อนส่งถึงผู้บริโภค บริษัทผลิตซอฟแวร์ (Software companies) ได้พัฒนาซอฟแวร์ที่ทำหน้าที่ปกป้องความปลอดภัยสำหรับอุปกรณ์โทรศัพท์เคลื่อนที่ เช่น McAfee Security Scan, Trend Micro Mobile Security, Symantec Client Security และ F-Secure Mobile Anti-Virus เป็นต้น

อย่างไรก็ตาม ผู้มีส่วนเกี่ยวข้องทั้งหมดจะต้องร่วมกันรับผิดชอบต่อความปลอดภัยของระบบปฏิบัติการโทรศัพท์เคลื่อนที่ และควรอยู่ในจุดที่จะสามารถตอบสนองต่อการป้องกันเหตุการณ์ที่มีผลต่อระบบความปลอดภัยได้ทันท่วงที (ตามหลักการข้อที่ 2 และ 3 ของแนวทางความปลอดภัยขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Security Guidelines)) โดยเฉพาะอย่างยิ่งผู้ผลิตและผู้ใช้จะต้องระวังต่อความเสี่ยงที่อาจเกิดขึ้นบนโทรศัพท์เคลื่อนที่อันเกิดจากไวรัส (ตามหลักการข้อที่ 1 ของแนวทางความปลอดภัยขององค์การ

---

[113] อ้างถึง Cousins, 2005.

เพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Security Guidelines)) ไม่ว่าผู้ใช้จะติดตั้งซอฟแวร์เพื่อป้องกันไวรัสบนโทรศัพท์เคลื่อนที่ (mobile viruses) ของตัวเองหรือไม่ ผู้ใช้ก็ควรจะระวังภัยเมื่อรับโปรแกรมต่างๆหรือเปิด MMS (Multimedia Message Service) ที่ไม่ทราบถึงแหล่งที่มา ในแนวทางยังแนะนำให้ปิดบริการ Bluetooth เมื่อไม่มีความจำเป็นต้องใช้บริการดังกล่าว ผู้ใช้ควรมีความระมัดระวังในเรื่องดังกล่าว และผู้ผลิตเองก็ควรจะต้องแจ้งภัยที่อาจเกิดขึ้นกับผลิตภัณฑ์โดยไวรัสให้แก่ผู้ใช้ด้วย[114]

แม้ว่าเครื่องมือต่อต้านไวรัสของ Pescatore and Girard (2005) จะสามารถกำจัดไวรัสได้ แต่ก็ไม่เพียงพอต่อการคุ้มครอง และที่ต้องการมากไปกว่านั้นก็คือ การสร้างความคุ้มครองไปยังระบบเครือข่ายด้วย ขณะเดียวกัน Hicks (2006) ได้กล่าวไว้ว่า ในอุตสาหกรรมเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ได้รับรู้ถึงความต้องการรูปแบบการรักษาความปลอดภัยในระบบคอมพิวเตอร์ (secure computing models) ที่สูงขึ้นสำหรับระบบการจัดการโทรศัพท์เคลื่อนที่ (mobile operating systems)

เมื่อการเจริญเติบโตของตลาดโทรศัพท์เคลื่อนที่สูงขึ้นอย่างรวดเร็ว บุคคลที่เกี่ยวข้องควรจะเริ่มประเมินความเสี่ยงที่จะมีผลต่อระบบความปลอดภัยของระบบ (ตามหลักการข้อที่ 6 ของแนวทางความปลอดภัยขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Security Guidelines)) การประเมินค่าความเสี่ยงช่วยในการเตรียมการป้องกันอันตรายที่อาจเกิดจากไวรัสซึ่งจะส่งผลต่อระบบปฏิบัติการ และยังช่วยพัฒนาเทคโนโลยีโทรศัพท์เคลื่อนที่ อีกทั้งยังสามารถเป็นผู้ช่วยในการเลือกการควบคุมที่เหมาะสมอีกด้วย

ดังนั้น ในประเด็นความเสี่ยงอันเกิดจากไวรัสและหนอนอินเตอร์เน็ต ผู้ดำเนินธุรกิจโทรศัพท์เคลื่อน (mobile phone operators) บางรายเริ่มที่จะพุ่งเป้าไปที่ระบบเครือข่าย (network) ตรวจรายละเอียดข้อความ เพื่อที่จะกลั่นกรองโปรแกรมที่ก่อให้เกิดความเสียหาย อุปกรณ์โทรศัพท์เคลื่อนที่ปัจจุบันบางรุ่น ได้มีการลงโปรแกรมป้องกันไวรัสก่อนส่งถึงผู้บริโภค บริษัทผลิตซอฟแวร์ (Software companies) ได้พัฒนาซอฟแวร์ที่ทำหน้าที่ปกป้องความปลอดภัยสำหรับอุปกรณ์โทรศัพท์เคลื่อนที่ อย่างไรก็ตาม ผู้มีส่วนเกี่ยวข้องทั้งหมดจะต้องร่วมกันรับผิดชอบต่อความปลอดภัยของระบบปฏิบัติการโทรศัพท์เคลื่อนที่ ควรจะเริ่มประเมินความเสี่ยงที่จะมีผลต่อระบบความปลอดภัยของระบบ และควรอยู่ในจุดที่จะสามารถตอบสนองต่อการป้องกันเหตุการณ์ที่มีผลต่อระบบความปลอดภัยได้ทันท่วงที โดยเฉพาะอย่างยิ่งผู้ผลิตและผู้ใช้จะต้องระวังต่อความเสี่ยงที่อาจเกิดขึ้นบนโทรศัพท์เคลื่อนที่อันเกิดจากไวรัส ไม่ว่าผู้ใช้จะติดตั้งซอฟแวร์

---

[114] อ้างถึง Nokia, 2005.

เพื่อป้องกันไวรัสบนโทรศัพท์เคลื่อนที่ (mobile viruses) ของตัวเองหรือไม่ แต่ทั้งนี้ ผู้ใช้ก็ควรจะระวังภัยเมื่อรับโปรแกรมต่างๆหรือเปิดข้อความมัลติมีเดีย (MMS) ที่ไม่ทราบถึงแหล่งที่มา และปิดบริการ Bluetooth เมื่อไม่มีความจำเป็นต้องใช้บริการดังกล่าว ผู้ใช้ควรมีความระมัดระวังในเรื่องดังกล่าว และผู้ผลิตเองก็ควรจะต้องแจ้งภัยที่อาจเกิดขึ้นกับผลิตภัณฑ์โดยไวรัสให้แก่ผู้ใช้ด้วย