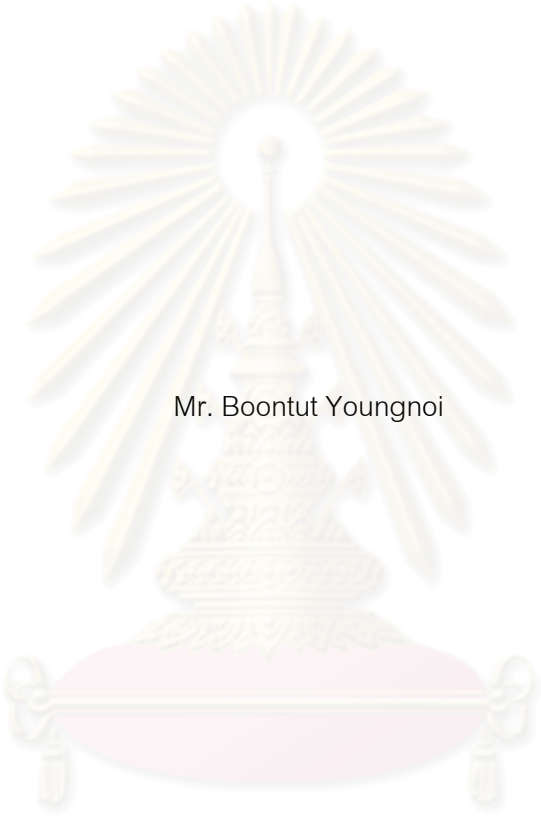
อาชญากรรมคอมพิวเตอร์ : ศึกษาข้อกฎหมายกรณีการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย

นายบุญทัศน์ ยังน้อย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2553

COMPUTER CRIME : A STUDY ON THE LEGAL ISSUES OF THE INTERNET PIRACY TROUGH WIRELESS NETWORK

Mr. Boontut Youngnoi



A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Laws Program in Laws
Faculty of Law
Chulalongkorn University
Academic Year 2010

หัวข้อวิทยานิพนธ์	อาชญากรรมคอมพิวเตอร์ : ศึกษาข้อกฎหมายกรณีการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย
โดย	นายบุญทัศน์ ยังน้อย
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ศาสตราจารย์วีระพงษ์ บุญโญภาส

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะนิติศาสตร์

(รองศาสตราจารย์ ดร.ศักดา ธนิตกุล)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ

(รองศาสตราจารย์ ดร.อภิรัตน์ เพ็ชรศิริ)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(ศาสตราจารย์วีระพงษ์ บุญโญภาส)

..... กรรมการภายนอกมหาวิทยาลัย

(รองศาสตราจารย์ ดร.ทวีเกียรติ มีนะกนิษฐ์)

..... กรรมการภายนอกมหาวิทยาลัย

(พันตำรวจเอกญาณพล ยั่งยืน)

บุญทัศน์ ยังน้อย : อาชญากรรมคอมพิวเตอร์ : ศึกษาข้อกฎหมายกรณีการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย (Computer Crime : A study on the legal issues of the internet piracy trough wireless network) อ. ที่ปรึกษาวิทยานิพนธ์หลัก : ศาสตราจารย์วีระพงษ์ บุญโญภาส, 159 หน้า.

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อที่จะศึกษาถึงข้อกฎหมายที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของผู้อื่น ทั้งกฎหมายที่ใช้บังคับในประเทศไทยและต่างประเทศ เนื่องจากการกระทำดังกล่าวเป็นการกระทำที่ส่งผลกระทบต่อประโยชน์ของเจ้าของเครือข่ายไร้สายและในบางกรณีเป็นสาเหตุของการก่ออาชญากรรมคอมพิวเตอร์ในรูปแบบอื่นด้วย แต่บทบัญญัติของกฎหมายที่ใช้บังคับอยู่ในปัจจุบันยังไม่มีความครอบคลุมเพียงพอ การวิจัยครั้งนี้จึงเป็นการหาคำตอบว่าการกระทำดังกล่าวควรจะมีรับผิดตามกฎหมายหรือไม่เพียงใด รวมทั้งศึกษาถึงหน้าที่ของเจ้าของเครือข่ายไร้สายที่ควรจะต้องดูแลระมัดระวังเครือข่ายไร้สายของตนมิให้ผู้อื่นมาใช้เป็นเครื่องมือในการกระทำความผิดด้วย

ผลการวิจัยพบว่า ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้คุ้มครองเครือข่ายไร้สายที่เจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ ส่งผลให้เกิดการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายได้ อีกทั้งการไม่ตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายจะส่งผลให้ผู้ลักลอบใช้เครือข่ายไร้สายกระทำความผิดโดยอาศัยเครือข่ายไร้สายเป็นเครื่องมือได้โดยง่าย ดังนั้น จึงสมควรที่จะต้องมีการบัญญัติกฎหมายเพื่อลงโทษผู้ลักลอบใช้เครือข่ายไร้สายของผู้อื่นโดยมีวัตถุประสงค์ในการกระทำความผิด และลงโทษเจ้าของเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของตนจนเป็นเหตุให้มีการกระทำความผิดขึ้นด้วย

สาขาวิชา นิติศาสตร์ ลายมือชื่อนิสิต Boontut Y.

ปีการศึกษา 2553 ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

5085997134 : MAJOR LAWS

KEYWORDS : ACCESS / COMPUTER / COMPUTER-RELATED CRIME ACT

BOONTUT YOUNGNOI : COMPUTER CRIME : A STUDY ON THE LEGAL ISSUES OF THE INTERNET PIRACY TROUGH WIRELESS NETWORK. ADVISOR : PROFESSOR VIRAPHONG BOONYOBHAS, 159 pp.

The purpose of this research is to study matters of law that are about stealing of surfing internet through the others' wireless including domestic and international law because this action affects the benefit of the wireless host and some case of this is the other causes of computer crime too. On the contrary, the present covenant which is used now does not cover enough. Therefore this research is to search for the answer that whether this action should be responsible in law and to study the duty of the wireless host who should take care of his own wireless by being careful the others who may use it as a tool of doing something wrong.

The result of the research found that the act of computer mistake of the year of 2550 does not cover the wireless of the host who does not set the measure to protect the access that cause the stealing of surfing internet through the others' wireless and it affect the smuggler to use the wireless as a tool easily. As a result, it should legislate the law to punish the smuggler who steal using the others wireless whose purpose is the mistake and to penalize the host of wireless who does not set the method of the protection of the access that cause the wrong action too.

Field of Study : Laws Student's Signature Boontut Y.

Academic Year : 2010 Advisor's Signature V. Boonyobhas

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้จะไม่สามารถสำเร็จลุล่วงไปได้ถ้าปราศจากความเมตตาและความช่วยเหลือจากผู้มีพระคุณดังต่อไปนี้

ศาสตราจารย์วีระพงษ์ บุญโญภาส อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ช่วยดูแลและให้คำปรึกษาตั้งแต่เริ่มต้นการวางโครงร่างวิทยานิพนธ์ แก้ไขโครงร่างวิทยานิพนธ์ รวมไปถึงการแบ่งบทของวิทยานิพนธ์ ชี้แนะวิธีการเขียนและเนื้อหาของวิทยานิพนธ์ อีกทั้งเมตตาให้เวลาผู้เขียนเข้าพบและซักถามเมื่อมีปัญหาเสมอมา

รองศาสตราจารย์ ดร.อภิรัตน์ เพ็ชรศิริ ประธานกรรมการสอบวิทยานิพนธ์ รองศาสตราจารย์ ดร.ทวีเกียรติ มีนะกนิษฐ์ และพันตำรวจเอกญาณพล ยั่งยืน กรรมการสอบวิทยานิพนธ์ ซึ่งได้กรุณาสละเวลาอันมีค่ายิ่งมาเป็นประธานกรรมการและกรรมการในการสอบวิทยานิพนธ์และให้คำแนะนำในการทำวิทยานิพนธ์

คุณฤทธิไกร ขัณฑวีระมงคล ผู้ก่อตั้งเวบไซต์ http://www.adslthailand.com ซึ่งได้กรุณาสละเวลาช่วยอธิบายวิธีการทำงานของระบบเครือข่ายไร้สายและมาตรการในการป้องกันเครือข่ายไร้สาย รวมทั้งตอบข้อซักถามของผู้เขียน

คุณภาสินี ไพศาลธนโชคและคุณสุภาณี สุขโชติที่ได้กรุณาช่วยผู้เขียนค้นหาข้อมูลที่เกี่ยวข้องกับการทำวิทยานิพนธ์ฉบับนี้ รวมทั้งได้ช่วยแปลบทความภาษาต่างประเทศและช่วยเหลือในการจัดพิมพ์วิทยานิพนธ์

ขอขอบพระคุณเจ้าหน้าที่ประจำหน่วยงานของคณะกรรมการสอบวิทยานิพนธ์ที่ได้ช่วยออกหมายนัดวันเวลาพบคณะกรรมการและขอขอบคุณเพื่อนๆทุกท่านที่ให้การสนับสนุนและให้กำลังใจเสมอมา

ผู้เขียนสำนึกในความเมตตา กรุณาของบุคคลต่างๆที่ได้กล่าวนามไว้แล้วข้างต้น และปิติยินดีเป็นอย่างยิ่งที่ได้มีโอกาสเผยแพร่เกียรติคุณของท่านให้ปรากฏไว้เป็นลายลักษณ์อักษรควบคู่กับวิทยานิพนธ์ฉบับนี้ต่อไป

เหนือสิ่งอื่นใด ผู้เขียนขอกราบขอบพระคุณบิดา มารดาซึ่งสนับสนุนผู้เขียนในทุกๆด้านเสมอมาทั้งให้ความรัก ความห่วงใยแก่ผู้เขียนมาโดยตลอด หากมีข้อบกพร่องประการในในเนื้อหาของวิทยานิพนธ์ฉบับนี้ผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

สารบัญ

หน้า

หน้า

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

พัฒนาการทางเทคโนโลยีสารสนเทศแม้ได้มีการนำมาประยุกต์ใช้และก่อให้เกิดประโยชน์มากมายแก่มนุษย์ก็ตาม ไม่ว่าจะเป็นด้านการทำงาน ด้านการศึกษาหรือระบบอำนวยความสะดวกต่างๆ แต่หากนำเทคโนโลยีสารสนเทศไปใช้ในทางมิชอบก็อาจก่อให้เกิดความเสียหายทางเศรษฐกิจอย่างรุนแรงหรือส่งผลกระทบที่ร้ายแรงแก่สังคมได้ คอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ถือเป็นเทคโนโลยีสารสนเทศชนิดหนึ่งที่ใช้สร้างประโยชน์อย่างแพร่หลาย แน่นอนว่าเมื่อคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ได้ถูกใช้ในทางเป็นประโยชน์ ในทางกลับกันก็มีผู้ที่กระทำความผิดโดยอาศัยคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เช่นกัน การกระทำดังกล่าวจึงอาจก่อให้เกิดอาชญากรรมรูปแบบใหม่จากการใช้คอมพิวเตอร์และเครือข่ายคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดหรือแสวงหาประโยชน์โดยมิชอบจากคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งการกระทำนี้ย่อมก่อให้เกิดภยันตรายหรือความเสียหายต่อระบบคอมพิวเตอร์ ระบบข้อมูลหรือระบบเครือข่ายซึ่งใช้ในการติดต่อสื่อสาร ซึ่งอาจเรียกอาชญากรรมชนิดนี้ได้ว่า อาชญากรรมคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์มีหลายรูปแบบ ไม่ว่าจะเป็นก่อกวนระบบคอมพิวเตอร์, การขโมยข้อมูลทางอินเทอร์เน็ตหรือการละเมิดลิขสิทธิ์ ปลอมแปลงรูปแบบหรือเลียนแบบระบบซอฟแวร์โดยมิชอบ เป็นต้น การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย มีลักษณะเป็นการกระทำความผิดทางคอมพิวเตอร์รูปแบบหนึ่ง เนื่องจากเป็นการลักลอบใช้ประโยชน์จากระบบคอมพิวเตอร์ของผู้อื่น จึงเป็นการกระทำที่ก่อให้เกิดความเสียหายต่อระบบเครือข่ายซึ่งใช้ในการติดต่อสื่อสารเนื่องจากการสื่อสารในเครือข่ายไร้สาย (Wireless LAN : WLAN) ระหว่างเครือข่ายไร้สายกับอุปกรณ์ไร้สายไม่ได้อาศัยสายสัญญาณอย่างที่ใช้อยู่กับระบบเครือข่ายใช้สาย (Wired LAN) โดยทั่วไป ดังนั้น อุปกรณ์ไร้สายที่อยู่ในบริเวณที่เครือข่ายไร้สายกระจายคลื่นวิทยุออกมาย่อมสามารถเชื่อมต่อกับเครือข่ายไร้สายได้ซึ่งการเชื่อมต่อเข้ากับเครือข่ายไร้สายนี้ เป็นการเชื่อมต่อเพื่อผ่านไปสู่ระบบอินเทอร์เน็ตภายนอกเครือข่ายไร้สาย

ปัญหาจึงมีอยู่ว่าบุคคลใดๆก็ตามสามารถนำอุปกรณ์ไร้สายเข้ามาเชื่อมต่อกับเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะได้ (unsecured wireless network) หากอุปกรณ์ไร้สายเครื่องนั้นอยู่ในระยะที่คลื่นสัญญาณไร้สายส่งไปถึง เมื่อการเชื่อมต่อเรียบร้อยแล้วบุคคลนั้นก็สามารถที่จะใช้บริการอินเทอร์เน็ตที่เจ้าของเครือข่ายไร้สายเป็นสมาชิกได้

โดยไม่ต้องเสียค่าใช้จ่ายแต่อย่างใด ในส่วนของการตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายนั้นต้องดำเนินการปรับแต่งค่าในอุปกรณ์กระจายสัญญาณไร้สาย โดยมีวิธีการที่ค่อนข้างเป็นเรื่องทางเทคนิค ซึ่งหากมิได้เป็นผู้ที่มีความเข้าใจในระบบเครือข่ายไร้สายเพียงพอก็อาจจะไม่ได้ตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของตนไว้ ดังนั้น การที่เจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะ โดยเฉพาะอย่างยิ่งในกรณีที่ผู้เจ้าของเครือข่ายไร้สายไม่มีความรู้ความเข้าใจในเรื่องนี้จึงไม่อาจถือได้ว่าเป็นการที่เจ้าของเครือข่ายไร้สายได้อนุญาตให้ผู้อื่นสามารถใช้บริการอินเทอร์เน็ตของเจ้าของเครือข่ายไร้สายได้

การลักลอบใช้เครือข่ายไร้สายของผู้อื่นนั้นทำให้ประสิทธิภาพโดยรวมของระบบเครือข่ายไร้สายด้อยลงเพราะมีผู้ใช้งานในระบบมาก แต่อย่างไรก็ตาม ถ้าเจ้าของเครือข่ายไร้สายพอจะทราบวิธีการตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของตนหรือทราบถึงอันตรายหรือความเสียหายที่จะเกิดขึ้นหากปล่อยให้ระบบเครือข่ายไร้สายของตนไม่มีมาตรการป้องกันการเข้าถึง กล่าวคือ เป็นระบบเครือข่ายที่ใครก็ตามสามารถเข้ามาใช้งานได้โดยง่าย การที่เจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะนั้นอาจถือได้ว่าเป็นกรณีที่เจ้าของเครือข่ายไร้สายให้ความยินยอมแก่ผู้อื่นในการเข้าถึงระบบคอมพิวเตอร์ของตน หากมีบุคคลใดเชื่อมต่อเข้าถึงระบบเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะ บุคคลนั้นจึงไม่ควรจะมีความรับผิดแต่อย่างใด ดังนั้น จึงสมควรต้องวิเคราะห์ว่าการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายในกรณีที่เจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยตนไม่ทราบถึงวิธีการตั้งมาตรการป้องกันและไม่ทราบถึงความเสียหายหรือประโยชน์ที่ตนอาจจะเสียไปหากมิได้ป้องกันเช่นนั้น เป็นการกระทำที่เป็นความผิดหรือไม่

ปัญหาที่ยิ่งไปกว่านั้น คือ หากเกิดกรณีที่มีผู้ลักลอบเข้าถึงระบบเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะโดยมิชอบโดยมีวัตถุประสงค์เพื่อใช้เครือข่ายไร้สายในการกระทำความผิด เช่น เข้าถึงระบบเครือข่ายไร้สายเพื่อทำการประกาศภาพอนาจารในเว็บไซต์หรือทำการฉ้อโกงผู้อื่นทางอินเทอร์เน็ต เจ้าของเครือข่ายไร้สายอาจจะถูกตั้งข้อสงสัยว่ามีส่วนเกี่ยวข้องในการกระทำความผิดร่วมกันกับผู้ลักลอบเข้าถึงระบบเครือข่ายไร้สายโดยไม่ชอบด้วย ซึ่งในกรณีที่มีผู้เข้าถึงระบบเครือข่ายไร้สายโดยไม่ชอบโดยมีวัตถุประสงค์ก่อให้เกิดความเสียหายแก่บุคคลอื่นโดยอาศัยเครือข่ายไร้สายที่เจ้าของไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะ เจ้าของเครือข่ายไร้สายก็อาจจะต้องมีความรับผิดเนื่องจากการไม่ตั้งมาตรการป้องกันการเข้าถึงนั้นด้วยหรืออาจจะถือได้ว่าเป็นผู้สนับสนุนในการกระทำความผิดนั้นโดยปริยาย

ปัญหาดังกล่าวนี้ ทั้งส่วนของผู้เข้าถึงระบบเครือข่ายไร้สายของผู้อื่นโดยมิชอบและเจ้าของเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะที่ละเลยไม่ตั้ง

มาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของตนจนเป็นเหตุให้มีผู้ลักลอบใช้เครือข่ายไร้สายในการกระทำความผิด ในปัจจุบันไม่อาจปรับใช้กับประมวลกฎหมายอาญาหรือพระราชบัญญัติที่มีโทษทางอาญา เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ เพราะพระราชบัญญัติฉบับดังกล่าวให้ความคุ้มครองเจ้าของเครือข่ายเฉพาะการที่มีผู้เข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับผู้เข้าถึงระบบคอมพิวเตอร์นั้นเท่านั้น รวมทั้งไม่มีบทบัญญัติที่กำหนดให้เจ้าของเครือข่ายไร้สายต้องตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะด้วยและเนื่องจากพระราชบัญญัติฉบับดังกล่าวได้มีการเปลี่ยนแปลงแก้ไขมาหลายครั้งก่อนจะประกาศใช้เป็นกฎหมาย ซึ่งแน่นอนว่าย่อมมีข้อถกเถียงในการบังคับใช้กฎหมาย รวมถึงอาจมีปัญหาในการตีความกฎหมายฉบับนี้ได้ในอนาคต ทั้งเป็นเรื่องใหม่และมีปัญหาเกี่ยวข้องกับเทคโนโลยีที่มีพัฒนาการไปอย่างรวดเร็วและต่อเนื่อง การบังคับใช้กฎหมายฉบับดังกล่าวกับกรณีปัญหาที่ยกมาข้างต้นจึงเป็นสิ่งที่น่าสนใจและเป็นเหตุจูงใจให้ข้าพเจ้าทำการศึกษาปัญหานี้

1.2 **สมมติฐานของการวิจัย**

การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายเป็นอาชญากรรมคอมพิวเตอร์รูปแบบหนึ่งที่มีแนวโน้มเกิดขึ้นมากและแทบจะไม่มีการรายงานการกระทำความผิด ซึ่งการกระทำความผิดในลักษณะนี้ก่อให้เกิดความเสียหายแก่เจ้าของเครือข่ายไร้สายหรือผู้ที่มีสิทธิใช้งานเครือข่ายไร้สายเนื่องจากทำให้ประสิทธิภาพโดยรวมของระบบลดลง และกฎหมายที่ใช้บังคับกับการกระทำความผิดนี้ในปัจจุบันอาจยังไม่สามารถใช้ได้กับทุกกรณีความผิด เช่น ไม่สามารถใช้บังคับได้กับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของเครือข่ายไร้สายที่มิได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะ รวมทั้งไม่มีการบัญญัติฐานความผิดเกี่ยวกับการลักลอบใช้บริการ (Theft of Services) เอาไว้เป็นพิเศษ อีกทั้ง การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายอาจนำไปสู่การกระทำความผิดทางคอมพิวเตอร์ในลักษณะอื่นๆได้อีก แต่อย่างไรก็ตาม เจ้าของเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะก็ควรจะมีความผิดจากการไม่ตั้งมาตรการป้องกันนี้ด้วย

1.3 **วัตถุประสงค์ของการวิจัย**

1. เพื่อให้ทราบถึงลักษณะของอินเทอร์เน็ต รวมถึงวิธีการให้บริการอินเทอร์เน็ตผ่านสัญญาณไร้สาย

2. เพื่อให้ทราบถึงลักษณะและประเภทของอาชญากรรมคอมพิวเตอร์และความเสียหายที่เกิดขึ้นจากอาชญากรรมคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งจากการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย รวมทั้งการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น

3. เพื่อแสดงให้เห็นถึงวิธีการกระทำความผิดเกี่ยวกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น รวมทั้งการบังคับใช้กฎหมายที่มีโทษทางอาญากับการกระทำดังกล่าว

4. เพื่อให้ทราบถึงแนวความคิดในการบังคับใช้กฎหมายที่มีโทษทางอาญาของต่างประเทศกับการกระทำความผิดที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น อีกทั้ง เพื่อให้ทราบถึงมาตรการในการจัดการความปลอดภัยของเครือข่ายไร้สายเพื่อหลีกเลี่ยงมิให้เกิดความเสียหายจากการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น

5. เพื่อให้ทราบถึงมาตรการในการจัดการความปลอดภัยของเครือข่ายไร้สายเพื่อหลีกเลี่ยงมิให้เกิดความเสียหายจากการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและลักลอบใช้บริการอินเทอร์เน็ตผ่านสัญญาณไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น

1.4 ขอบเขตของการวิจัย

อาชญากรรมคอมพิวเตอร์ก่อให้เกิดความเสียหายและเป็นอันตรายแก่ระบบต่างๆ ของประเทศไม่ว่าจะเป็นระบบความมั่นคง เศรษฐกิจ สังคมและการเมือง อาชญากรรมคอมพิวเตอร์มีอยู่ด้วยกันหลายประเภท หนึ่งในจำนวนนั้นก็คือ การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย บุคคลที่จะกระทำความผิดจะได้รับประโยชน์จากการกระทำนี้ซึ่งไม่ใช่แต่ในประเทศไทยเท่านั้น ในต่างประเทศก็มีเหตุการณ์เหล่านี้เกิดขึ้น

การวิจัยฉบับนี้ จะได้ทำการศึกษาอาชญากรรมคอมพิวเตอร์เฉพาะในแง่ที่เกี่ยวกับกรณีการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย รวมถึงการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น ซึ่งการวิจัยจะ

ประกอบด้วยการศึกษาลักษณะทั่วไปของอินเทอร์เน็ต ลักษณะของเครือข่ายไร้สาย (Wireless LAN : WLAN) และเครือข่ายใช้สาย (Wired LAN) การใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย การใช้และเปลี่ยนค่า IP Address ลักษณะการกระทำความผิดที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น กับกฎหมายที่เกี่ยวข้องต่างๆของประเทศไทย และได้วิจัยเปรียบเทียบกับกฎหมายที่เกี่ยวกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่นในต่างประเทศ รวมทั้งได้ศึกษาถึงมาตรการต่างๆในการจัดการความปลอดภัยของเครือข่ายไร้สาย เพื่อที่จะคุ้มครองมิให้เกิดความเสียหายในการกระทำความผิดดังกล่าว อันเป็นวัตถุประสงค์ของการวิจัยฉบับนี้

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ทราบถึงลักษณะของอินเทอร์เน็ต รวมถึงวิธีการให้บริการอินเทอร์เน็ตผ่านสัญญาณไร้สาย

2. ทำให้ทราบถึงลักษณะและประเภทของอาชญากรรมคอมพิวเตอร์และความเสียหายที่เกิดขึ้นจากอาชญากรรมคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งจากการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น

3. แสดงให้เห็นถึงวิธีการกระทำความผิดเกี่ยวกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น รวมทั้งการบังคับใช้กฎหมายที่มีโทษทางอาญากับการกระทำดังกล่าว

4. ทำให้ทราบถึงแนวความคิดในการบังคับใช้กฎหมายที่มีโทษทางอาญาของต่างประเทศกับการกระทำความผิดที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น

5. ทำให้ทราบถึงมาตรการในการจัดการความปลอดภัยของเครือข่ายไร้สายเพื่อหลีกเลี่ยงมิให้เกิดความเสียหายจากการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและลักลอบใช้บริการอินเทอร์เน็ตผ่านสัญญาณไร้สายโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น

1.6วิธีดำเนินการวิจัย

เป็นการวิจัยแบบเอกสาร โดยการศึกษาวิเคราะห์ข้อมูลจากเอกสารเป็นหลัก

บทที่ 2
บทวิเคราะห์ศัพท์

การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายมีลักษณะเป็นการกระทำที่เกี่ยวข้องกับการใช้เทคโนโลยีและอินเทอร์เน็ตในการกระทำความผิด ดังนั้นจึงสมควรที่จะต้องทราบถึงลักษณะการทำงานของระบบอินเทอร์เน็ตซึ่งแยกได้เป็นบริการอินเทอร์เน็ตแบบใช้สายสัญญาณในการนำข้อมูลและบริการอินเทอร์เน็ตแบบไม่ใช้สายสัญญาณในการนำข้อมูล รวมถึงเทคโนโลยีต่างๆที่เกี่ยวข้องกับการบริการอินเทอร์เน็ต ทั้งนี้ เมื่อทราบถึงลักษณะของการทำงานของระบบอินเทอร์เน็ต ก็จะเข้าใจรูปแบบของกระทำความผิดที่เกิดขึ้นได้

การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายในบางครั้งผู้กระทำได้กระทำโดยมีเจตนาจะใช้เครือข่ายไร้สายของผู้อื่นในการกระทำความผิดซึ่งพยานหลักฐานที่จะใช้ในการพิสูจน์การกระทำความผิดในกรณีนี้ได้แก่ไอพีแอดเดรส (IP Address) ซึ่งในกรณีของ IP Address ประเด็นที่สำคัญที่สุดก็จะเป็นประเด็นที่เกี่ยวข้องกับการแปลงค่า IP Address ดังนั้น ในบทที่ 2 ซึ่งเป็นบทวิเคราะห์ศัพท์ ผู้เขียนก็จะได้อธิบายให้เห็นถึงประเภทของ IP Address ที่ใช้ในการบริการอินเทอร์เน็ต และการแปลงค่า IP Address

2.1 บริการอินเทอร์เน็ต

อินเทอร์เน็ต เป็นระบบเครือข่ายคอมพิวเตอร์ใหญ่ที่สุดในโลก ซึ่งเกิดจากการที่ระบบคอมพิวเตอร์เครือข่ายย่อยๆ หลายๆเครือข่ายรวมตัวกัน เป็นระบบเครือข่ายขนาดใหญ่ ในอีกความหมายหนึ่งหมายถึงการที่คอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไป สามารถติดต่อสื่อสารซึ่งกันและกันได้โดยผ่านสายเคเบิ้ลหรือสายโทรศัพท์ ดาวเทียม ฯลฯ การติดต่อนั้นจะเป็นการแลกเปลี่ยนข้อมูลซึ่งกันและกัน หรือใช้อุปกรณ์ร่วมกัน เช่น ใช้เครื่องพิมพ์ (Printer) หรือ CD-Rom ร่วมกัน เราเรียกพฤติกรรมของคอมพิวเตอร์ลักษณะนี้ว่า เครือข่าย (Network) ซึ่งเมื่อมีจำนวนคอมพิวเตอร์ในเครือข่ายมากขึ้น และมีการเชื่อมโยงกันไปทั่วโลก จนกลายเป็นเครือข่ายขนาดใหญ่ เราเรียกสิ่งนี้ว่า อินเทอร์เน็ต นั่นเอง

การประยุกต์ใช้งานอินเทอร์เน็ตในปัจจุบันทำได้หลากหลาย อาทิเช่น ไปรษณีย์อิเล็กทรอนิกส์ หรือ อีเมล์ (e-Mail) , สนทนา (Chat), อ่านหรือแสดงความคิดเห็นในเว็บบอร์ด (Webboard), การติดตามข่าวสาร, การสืบค้นข้อมูลหรือการค้นหาข้อมูล, การชม หรือซื้อสินค้า

ออนไลน์ , การดาวน์โหลดเกม เพลง ไฟล์ข้อมูล, การติดตามข้อมูล ภาพยนตร์ รายการบันเทิงต่างๆ ออนไลน์, การเล่นเกมคอมพิวเตอร์ออนไลน์, การเรียนรู้ออนไลน์ (e-Learning), การประชุมทางไกลผ่านอินเทอร์เน็ต (Video Conference), โทรศัพท์ผ่านอินเทอร์เน็ต (VoIP), การอัพโหลดข้อมูลหรืออื่นๆ

แนวโน้มล่าสุดของการใช้อินเทอร์เน็ตคือการใช้อินเทอร์เน็ตเป็นแหล่งพบปะสังสรรค์เพื่อสร้างสังคมออนไลน์ (Social Network) ซึ่งพบว่าปัจจุบันเว็บไซต์ที่เกี่ยวข้องกับกิจกรรมดังกล่าวกำลังได้รับความนิยมอย่างแพร่หลาย ไม่ว่าจะเป็น facebook, twitter, hi5 และการใช้เริ่มมีการแพร่ขยายเข้าไปสู่การใช้อินเทอร์เน็ตผ่านโทรศัพท์มือถือ (Mobile Internet) มากขึ้น เนื่องจากเทคโนโลยีปัจจุบันสนับสนุนให้การเข้าถึงเครือข่ายผ่านโทรศัพท์มือถือทำได้ง่ายขึ้นมาก

สำหรับการเชื่อมต่อเพื่อเข้าใช้บริการอินเทอร์เน็ตมีทั้งการเชื่อมต่อระบบอินเทอร์เน็ตโดยอาศัยตัวนำเป็นสายสัญญาณและแบบไร้สาย การเชื่อมต่อกันของแต่ละเครือข่ายภายในเครือข่ายอินเทอร์เน็ตนั้น จะมีองค์กรหรือหน่วยงานที่คอยให้บริการด้านอินเทอร์เน็ตที่เรียกว่า “ISP (Internet Service Provider)” ที่คอยให้บริการแก่องค์กรหรือผู้ใช้ที่ต้องการใช้งานอินเทอร์เน็ตโดย ISP มีขนาดตั้งแต่ระดับประเทศจนถึงระดับท้องถิ่น เช่น ISP ระดับประเทศ (National ISP) ซึ่งให้บริการเชื่อมต่อกับ ISP ระหว่างประเทศและดูแล ISP ภายในประเทศ, ISP ระดับภูมิภาค (Regional ISP) ที่ให้บริการในแต่ละภูมิภาคและ ISP ระดับท้องถิ่น (Local ISP) ที่ให้บริการในระดับเมืองหรือเฉพาะในท้องถิ่น ในแต่ละประเทศต่างก็มีผู้ให้บริการเครือข่ายอินเทอร์เน็ต ซึ่งจะคอยดูแลและจัดการเครือข่ายอินเทอร์เน็ตทั้งประเทศหรือเฉพาะส่วนภูมิภาค[1]

ในประเทศไทยมีรายนามผู้ให้บริการอินเทอร์เน็ต (ISP) ดังต่อไปนี้[2]

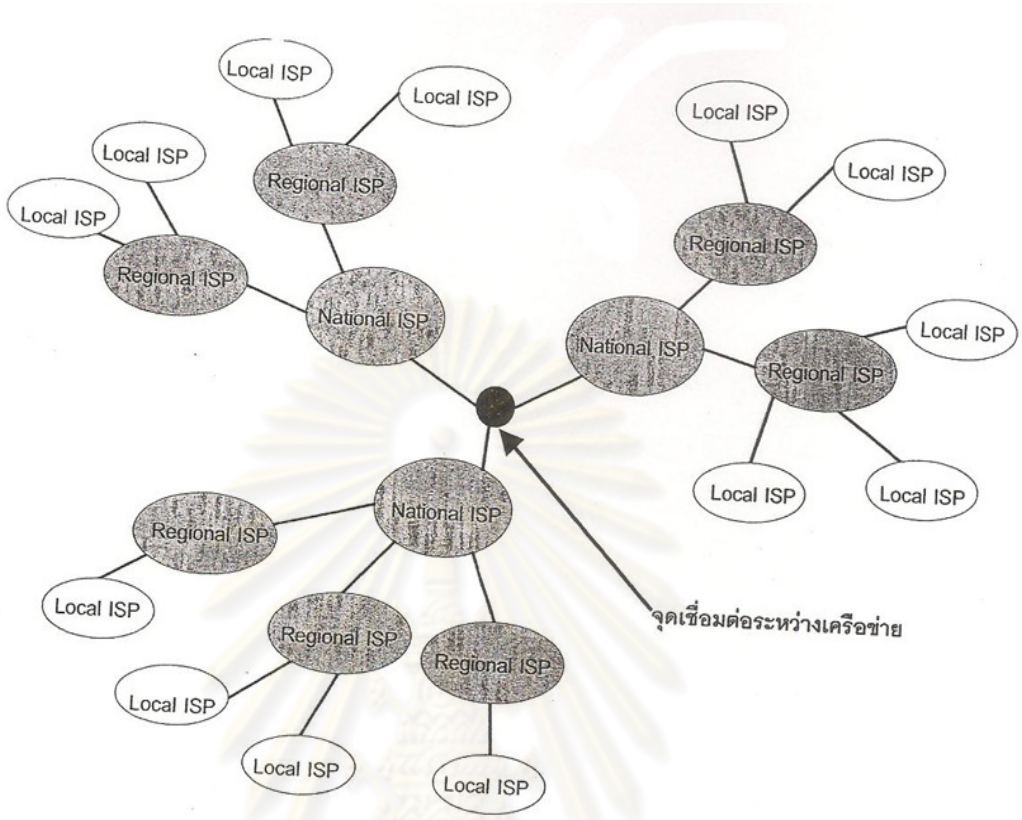
- บริษัท กสท. โทรคมนาคม จำกัด (มหาชน) (**CAT Telecom Public Co., Ltd.**)
- บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) (**Internet Thailand Public Company Limited**)

---

[1] สุธี พงศาสกุลชัยและณรงค์ ล่ำดี, <u>การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์</u> (กรุงเทพมหานคร : เคทีพี คอมพ์ แอนด์ คอนซัลท์, 2551), หน้า 239-242

[2] อาณัติ รัตนถิรกุล, “รายนามศูนย์บริการอินเทอร์เน็ต (ISP) ในไทย,” [Online] แหล่งที่มา : http://www.arnut.com/isp.php [วันที่ 3 สิงหาคม 2553]

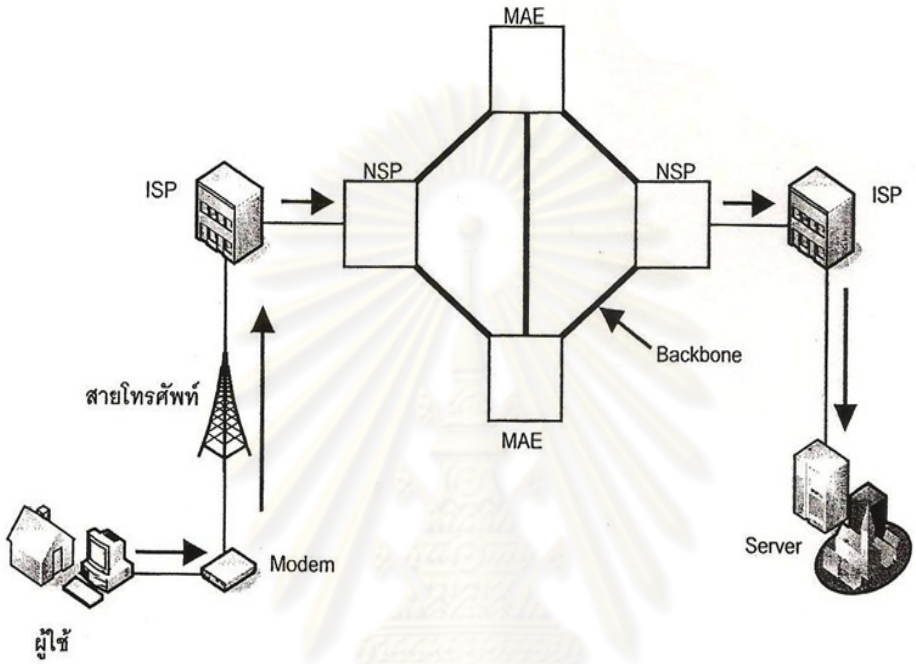
- บริษัท แปซิฟิค อินเทอร์เน็ต (ประเทศไทย) จำกัด (World Net & Services Co.,Ltd.)
- บริษัท จัสมิน อินเตอร์เนต จำกัด (Jasmine Internet Co, Ltd.)
- บริษัท เอเน็ต จำกัด (Anet Co.,Ltd.)
- บริษัท สามารถอินโฟเนต จำกัด (Samart InfoNet Co., Ltd.)
- บริษัท ทีทีแอนด์ที จำกัด (มหาชน) (Triple T Global Net)
- KIRZ Company Limited
- บริษัท โอทาโร จำกัด (OTARO Company Limited)
- บริษัท อินเตอร์เนต โซลูชั่น แอนด์ เซอร์วิส โพรวายเดอร์ จำกัด (Internet Service Provider Co., Ltd. (ISSP))
- PROEN Internet
- Proimage Engineering and Communication Co., Ltd
- Far East Internet Co., Ltd
- CSLoxinfo
- บริษัท ทรู อินเทอร์เน็ต จำกัด (TRUE Internet)
- บริษัท เค เอส ซี คอมเมอร์เชียล อินเตอร์เนต จำกัด (KSC)
- บริษัท ทีโอที จำกัด (มหาชน) (TOTWEB)
- Advanced Datanetwork Communications Co.,Ltd (ADC)
- บริษัท ชมะนันทน์เวิล์ดเน็ต จำกัด (Chomanan WorldNet. Name Inc CWN)



ในส่วนของการทำงานของระบบเครือข่ายอินเทอร์เน็ต เมื่อผู้ใช้งานป้อนชื่อของเว็บไซต์ที่ต้องการเข้าชมหรือต้องการใช้บริการอินเทอร์เน็ตในรูปแบบใดๆก็ตาม การทำงานของระบบทั้งหมดจะเริ่มต้นที่ผู้ใช้บริการโดยการส่งข้อมูลจะส่งผ่านผู้ดูแลหรือผู้ให้บริการ (ISP) นั่นเอง

ผู้ใช้บริการจำเป็นต้องมีอุปกรณ์ที่ใช้ในการเชื่อมต่อเข้ากับเครือข่ายอินเทอร์เน็ต เช่น ในกรณีระบบอินเทอร์เน็ตที่ใช้โมเด็ม (Modem) ทำการเชื่อมต่อซึ่งผู้ใช้บริการจำเป็นต้องเป็นสมาชิกของผู้ให้บริการ (ISP) เสียก่อน ภายหลังจากที่ผู้ใช้บริการหมุน Modem เชื่อมต่อระบบอินเทอร์เน็ตกับ ISP แล้ว เมื่อผู้ใช้บริการต้องการเข้าเว็บไซต์เครื่องคอมพิวเตอร์ก็จะส่งคำร้องขอไปยังเครื่องเซิร์ฟเวอร์ (Server) ที่เก็บข้อมูลของเว็บไซต์ดังกล่าวอยู่ ข้อมูลจะเริ่มเดินทางจากเครื่องผู้ใช้บริการโดยมี Modem ทำหน้าที่ในการเชื่อมต่อเครื่องคอมพิวเตอร์กับเครือข่ายอินเทอร์เน็ตผ่านทางสายโทรศัพท์ ข้อมูลจากผู้ใช้บริการจะเดินทางไปยังผู้ให้บริการหรือ ISP ซึ่งข้อมูลดังกล่าวจะอยู่ในรูปแบบของแพ็กเกจข้อมูล (Data Packet) โดย ISP จะเป็นตัวกลางในการเชื่อมต่อสัญญาณข้อมูลจากผู้ใช้ต้นทางและทำการส่งไปยังปลายทางผ่านไปยังผู้ให้บริการเครือข่ายหรือ NSP (Network Service Provider) ซึ่งจะเชื่อมต่อกับอินเทอร์เน็ตเครือข่ายหลัก (Internet Backbone) และจะคอยจัดการหาเส้นทางให้ข้อมูลจากต้นทางไปยังปลายทางได้อย่างถูกต้อง

แพ็กเกจข้อมูลดังกล่าวจะเดินทางผ่าน Backbone ตามเส้นทางที่ NSP จัดเตรียมไว้ ในระหว่างนั้นจะมีส่วนที่รับข้อมูลต่อจาก NSP ก็คือ MAE (Metropolitan Area Exchange) ที่จะเชื่อมต่อกับ Backbone และ MAE อื่น ก่อนจะส่งข้อมูลไปยัง ISP ในฝั่งที่ให้บริการเครื่อง Server ปลายทางอยู่ ดังปรากฏตามรูปดังต่อไปนี้



แสดงกระบวนการส่งข้อมูลผ่านเครือข่ายอินเตอร์เน็ต

หลังจากที่แพ็กเกจข้อมูลเดินทางมาถึงยัง ISP ปลายทางแล้ว ก็จะถูกจัดส่งไปยังเครื่อง Server ที่เก็บข้อมูลของเว็บไซต์ดังกล่าวไว้ ซึ่งอาจเป็นเครื่อง Server ของภายในองค์กรนั้น หรืออาจเป็นเครื่อง Server ของผู้ให้บริการจัดเก็บข้อมูลเว็บไซต์ที่เรียกว่า “เว็บโฮสติ้ง (Web Hosting)” ก็ได้ เมื่อปลายทางได้รับการร้องขอเพื่อเปิดเว็บไซต์ ก็จะส่งข้อมูลของเว็บไซต์ต่างๆ กลับไปยังเครื่องผู้ใช้เพื่อให้ประมวลผลและแสดงหน้าเว็บไซต์ดังกล่าว ดังนั้น จะเห็นได้ว่าระบบการส่งข้อมูลจากผู้ใช้บริการไปยังผู้ให้บริการปลายทาง (Web Hosting) และการส่งข้อมูลสนองตอบจากผู้ให้บริการไปยังผู้ใช้บริการเป็นไปตามที่กล่าวไว้ข้างต้น ซึ่งทั้งระบบการใช้บริการอินเทอร์เน็ตแบบใช้สายสัญญาณและแบบไร้สายจะแตกต่างกันเพียงการใช้สายสัญญาณเป็นตัวนำข้อมูลหรือไม่เท่านั้น

2.1.1 บริการอินเทอร์เน็ตแบบใช้สายสัญญาณ

รูปแบบการบริการอินเทอร์เน็ตบางประเภททุกช่วงของการขนส่งข้อมูลจะใช้สายสัญญาณเป็นตัวนำข้อมูลทั้งสิ้น เราเรียกการสื่อสารข้อมูลประเภทนี้ว่า สื่อแบบมีสาย (Guided Media) ซึ่งสายสัญญาณที่ใช้จะมี 3 ประเภทคือ สายคู่ตีเกลียว (Twisted – Pair Cable) สายโคแอ็กเชียล (Coaxial Cable) สายไฟเบอร์ออปติก (Fiber – Optic Cable) บริการอินเทอร์เน็ตแต่ละประเภทจะใช้สายสัญญาณประเภทใดขึ้นอยู่กับรูปแบบของการให้บริการซึ่งมีดังต่อไปนี้

2.1.1.1 บริการอินเทอร์เน็ตที่ใช้ Modem 56 k[3]

บริการอินเทอร์เน็ตประเภทนี้ค่อนข้างจะไม่เป็นที่นิยมในปัจจุบันแล้ว เนื่องจากมีเทคโนโลยีอินเทอร์เน็ตความเร็วสูงมาแทนที่ (เทคโนโลยีอินเทอร์เน็ตบรอดแบนด์) การใช้บริการอินเทอร์เน็ตที่ใช้ Modem 56 k ผู้ใช้บริการจะต้องติดต่อผู้ให้บริการ (ISP) เพื่อขอใช้บริการซึ่งมีทั้งประเภทคิดค่าบริการรายเดือนหรือคิดค่าบริการเป็นรายชั่วโมง เมื่อขอรับบริการแล้ว ผู้ใช้บริการจะได้หมายเลขประจำตัว (Username) และรหัสผ่าน (Password) สำหรับเชื่อมต่อกับผู้ให้บริการ เมื่อติดตั้งอุปกรณ์ต่างๆเรียบร้อยพร้อมใช้อินเทอร์เน็ตแล้ว ผู้ใช้บริการจะหมุน Modem ติดต่อไปยังผู้ให้บริการอินเทอร์เน็ต (ISP) ซึ่งทางฝั่งผู้ให้บริการก็จะมี Modem อีกตัวติดตั้งเข้ากับเครื่อง Server อยู่ โดยการส่งข้อมูลจะเป็นการส่งข้อมูลผ่านสายโทรศัพท์[4]

---

[3] อรรณพ ขันธิกุลและอำนาจ มีมงคล, ติดตั้งและใช้งาน Hi Speed Internet (นนทบุรี : ไอดีซีฯ, 2549), หน้า 29-31

[4]สายโทรศัพท์เป็นสายนำสัญญาณประเภทสายคู่ตีเกลียว (Twisted – Pair Cable) ซึ่งเป็นสายที่ประกอบด้วยลวดทองแดง 2 เส้นทำหน้าที่เป็นสื่อทางไฟฟ้า มีฉนวนหุ้มลวดทองแดงเอาไว้และสายทั้งสองนั้นมาพันเป็นเกลียว สายหนึ่งจะเป็นสายนำสัญญาณข้อมูล อีกสายหนึ่งเป็นสายกราวน์ โดยปกติแล้วสายคู่ตีเกลียว (Twisted – Pair Cable) จะมีการใช้งานกันอยู่ทั่วๆไปเป็นแบบ unshielded twisted – pair (UTP) ซึ่งสายโทรศัพท์จะใช้สายคู่ตีเกลียวประเภทนี้ สายคู่ตีเกลียวอีกประเภทหนึ่ง คือ shielded twisted – pair (STP) ซึ่งจะแตกต่างตรงที่มีขดลวดโลหะมาหุ้มอีกชั้นหนึ่ง (อ้างใน จักกริช พฤษการ, การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Communication and Networking) (กรุงเทพมหานคร : ท้อป, 2549), หน้า 122)

ในส่วนการทำงานของ Modem Modem ของทั้ง 2 ฝ่ายจะพยายามเชื่อมต่อกันด้วยมาตรฐานที่ดีที่สุดที่รองรับและจะคอยตรวจสอบสภาพสายโทรศัพท์ว่าดีหรือไม่ก่อนที่จะเชื่อมต่อ ซึ่งการเชื่อมต่อทั่วๆไปจะอยู่ที่ 33.6-53 kbps ซึ่งเมื่อเชื่อมต่อสำเร็จแล้วผู้ใช้บริการก็สามารถใช้บริการอินเทอร์เน็ตได้

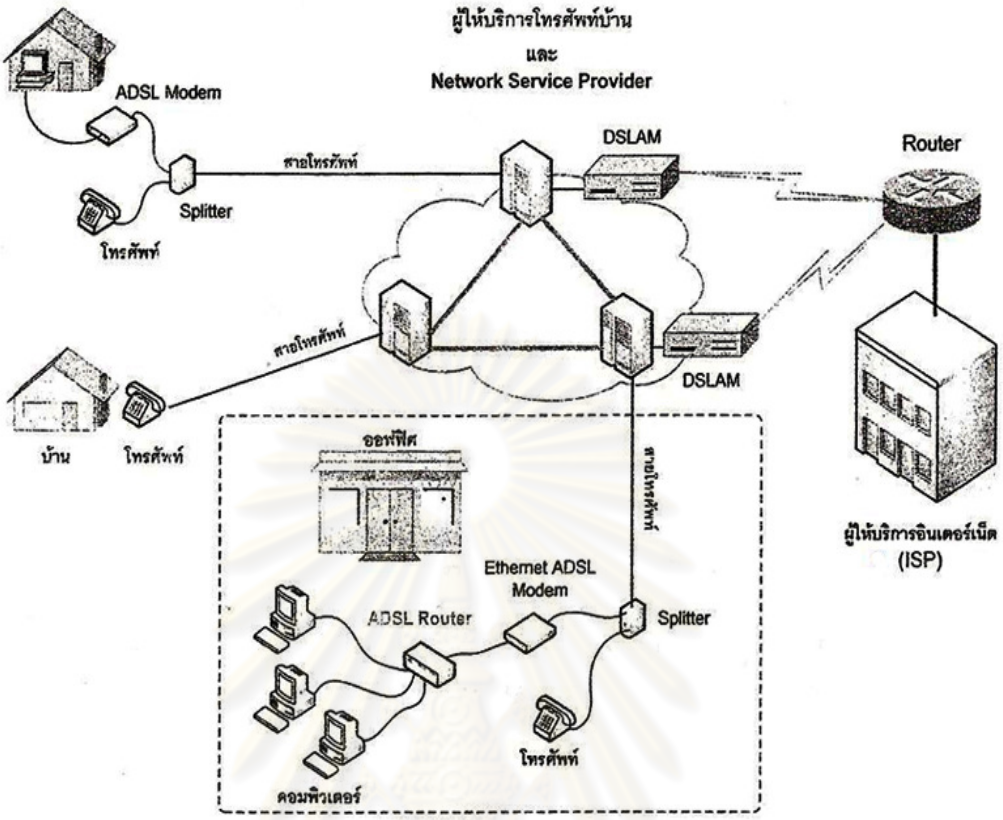
2.1.1.2 **บริการอินเทอร์เน็ต** DSL (Digital Subscriber Loop) **ผ่านสายโทรศัพท์**

บริการอินเทอร์เน็ตประเภทนี้ เป็นเทคโนโลยีอินเทอร์เน็ตความเร็วสูงผ่านสายโทรศัพท์ซึ่งมีความเร็วมากกว่าใช้ Modem 56 k ถึง 140 เท่า ความแตกต่างอยู่ที่ Modem 56 k ทำงานในช่วงความถี่ 300 - 400 เฮิรตซ์ ซึ่งเป็นความถี่เสียงพูด ส่วนระบบ DSL ทำงานอยู่ในช่วง 24 - 1,104 กิโลเฮิรตซ์ การใช้บริการอินเทอร์เน็ตในระบบ DSL ผู้ใช้บริการจะสามารถใช้โทรศัพท์ในระหว่างที่ใช้บริการอินเทอร์เน็ตได้ เพราะความถี่ของระบบโทรศัพท์อยู่ในช่วง 0 – 4 กิโลเฮิรตซ์ ซึ่งเป็นคนละย่านความถี่กับระบบ DSL แต่อย่างไรก็ตาม จะต้องติดตั้งสปลิตเตอร์ (Splitter) ซึ่งเป็นอุปกรณ์ที่ใช้เพื่อแยกความถี่ของระบบโทรศัพท์ออกจากความถี่ของระบบ DSL เสียก่อน

สิ่งที่ต้องคำนึงถึงในการติดตั้งระบบอินเตอร์เน็ตแบบ DSL ก็คือ

1. ต้องตรวจสอบว่าสถานที่ที่ติดตั้งอยู่ในเขตพื้นที่ให้บริการระบบโทรศัพท์แบบ DSL หรือไม่
2. บัญชีผู้ใช้อินเตอร์เน็ตจากผู้ให้บริการอินเตอร์เน็ตในแบบ DSL
3. การเชื่อมต่อต้องใช้ DSL Modem ในการเชื่อมต่อ
4. ต้องติดตั้ง Ethernet Adapter Card หรือ Lan Card ไว้ที่เครื่องคอมพิวเตอร์ที่ใช้ในการเชื่อมต่ออินเตอร์เน็ตด้วย

ความจริงแล้ว DSL Modem นั้นก็ทำงานไม่ได้ต่างไปจาก Modem 56 k แบบเดิมเท่าใดนัก เทคโนโลยีตัวนี้เกิดขึ้นมาได้เมื่อมีการพัฒนาวงจรอิเล็กทรอนิกส์ความเร็วสูงที่สามารถทำงานได้ดีกว่าแบบเดิมหลายร้อยเท่า กล่าวได้ว่า DSL Modem นั่นก็คือ Modem 56 k ธรรมดาจำนวน 224 ตัวที่ทำงานขนานกันไปในด้านดาวน์สตรีม (การดาวน์โหลดข้อมูล) และอีก 25 ตัวในฝั่งอัพสตรีม (การอัพโหลดข้อมูล)



จากรูปในการทำงานของระบบ DSL นั้นจะประกอบไปด้วย[5] ส่วนที่สำคัญคือสายโทรศัพท์สำหรับรับและส่งข้อมูล DSL Modem ที่ใช้ต่อเข้ากับคอมพิวเตอร์ ทางด้านชุมสายก็จะมี Modem ไว้รองรับ โดยมีอุปกรณ์อีกตัวเรียกว่า “DSLAM (Digital subscriber line access multiplexer)” หรือตัวรวมสัญญาณ DSL หลายๆเส้นเข้าไปในเครือข่ายคอมพิวเตอร์ เพื่อส่งไปยังผู้ให้บริการอินเทอร์เน็ต (ISP)

ในส่วนนี้จะเป็นหน้าที่ของผู้ให้บริการโครงข่าย (Network Service Provider) ตัวอย่างเช่น ถ้าคู่สายของทรูก็จะมีบริษัท ทรู มัลติมีเดีย รับผิดชอบโครงข่าย DSL นี้ จากนั้นก็จะเชื่อมต่อเข้ากับ ISP

---

[5] อรรณพ ขันธิกุล และ อำนาจ มีมงคล, ติดตั้งและใช้งาน Hi Speed Internet ,หน้า 127-174

ในโครงข่ายอินเทอร์เน็ตความเร็วสูงแบบ DSL นั้นจะไม่ได้มีการจัดสรรแบนด์วิธ[6] (Bandwidth) ให้กับผู้ใช้งานตามปริมาณการใช้งานจริงดังเช่นการใช้บริการเครือข่ายวงจรเช่า (Leased Line) แต่ ระบบ DSL นั้นจะเป็นบริการที่มีการแชร์กันใช้งานเนื่องจากเป็นบริการราคาถูก สายสัญญาณที่ใช้เชื่อมโยงจากชุมสายไปยังผู้ให้บริการอินเทอร์เน็ต (ISP) จึงมีการแชร์กันใช้งาน เพื่อประหยัดค่าใช้จ่าย ปัญหาอินเทอร์เน็ตช้าก็เกิดจากการแชร์กันใช้งานในโครงข่าย DSL

ในส่วนของอุปกรณ์ DSL Modem เป็นอุปกรณ์ที่ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ 1 เครื่อง เชื่อมไปยังระบบ DSL ของผู้ให้บริการโดยผ่านคู่สายโทรศัพท์ ทำให้คอมพิวเตอร์ของผู้ใช้บริการสามารถใช้งานอินเทอร์เน็ตความเร็วสูงได้ในลักษณะผู้ใช้คนเดียว (Single User) เท่านั้น

หลักการทำงานของ DSL Modem คือ จะรับข้อมูลดิจิทัลจากเครื่องคอมพิวเตอร์ จากนั้นก็จะนำมาโมดูเลต (Modulate) กลายเป็นสัญญาณอะนาล็อกเพื่อให้ส่งสัญญาณไปได้ไกลยิ่งขึ้น แล้วส่งสัญญาณอินเทอร์เน็ตความเร็วสูงนี้ผ่านคู่สายโทรศัพท์ไปยังอุปกรณ์ DSLAM ที่ตั้งอยู่ ณ ชุมสายโทรศัพท์ปลายทาง

ณ ชุมสายโทรศัพท์ก็จะทำในทางกลับกันคือ DSL Modem ที่นี่จะดีโมดูเลต (Demodulate) เปลี่ยนสัญญาณอะนาล็อกที่ได้รับเป็นสัญญาณดิจิทัลส่งให้อุปกรณ์เครือข่ายในชุมสายโทรศัพท์อีกทีหนึ่ง ชุมสายก็จะส่งข้อมูลไปให้กับผู้ให้บริการอินเทอร์เน็ต (ISP)

ในส่วนบริการอินเทอร์เน็ตในระบบ DSL ยังมีอุปกรณ์อีกชนิดหนึ่ง คือ DSL Router หรือที่รู้จักกันอีกชื่อก็คือ “บรอดแบนด์เราท์เตอร์ (Broadband Router)” เป็นอุปกรณ์ค้นหาเส้นทางรับ-ส่งข้อมูลบนเครือข่ายอินเทอร์เน็ตความเร็วสูง และจะคอยรับการร้องขอเชื่อมต่อไปยัง

---

[6] Bandwidth คือ ความกว้างของช่องทางในการรับ-ส่งข้อมูล เป็นคำที่ใช้วัดความเร็วในการส่งข้อมูลของอินเทอร์เน็ต ซึ่งโดยมากมักวัดความเร็วของการส่งข้อมูลเป็น bps (bit per second) , Mbp (bps*1000000) เช่น Bandwidth ของการใช้สายโทรศัพท์ในประเทศไทย เท่ากับ 14.4 Kbps,Bandwidth ของสายส่งข้อมูลของ KSC ที่ใช้ในการเชื่อมต่อกับสหรัฐอเมริกาเท่ากับ 2 Mbps เป็นต้น (อ้างใน วิกิพีเดีย สารานุกรมเสรี, “แบนด์วิดท์” [ออนไลน์], 13 กันยายน 2553. แหล่งที่มา :

http://th.wikipedia.org/wiki/%E0%B9%81%E0%B8%9A%E0%B8%99%E0%B8%94%E0%B9%8C%E0%B8%A7%E0%B8%B4%E0%B8%94%E0%B8%97%E0%B9%8C)

อินเทอร์เน็ต จึงสามารถแชร์อินเทอร์เน็ตความเร็วสูงให้แก่เครื่องคอมพิวเตอร์ลูกข่ายจึงเหมาะสำหรับบ้าน สำนักงานขนาดเล็กจนถึงขนาดกลาง รวมถึงร้านอินเทอร์เน็ตคาเฟ่ที่มีเครื่องคอมพิวเตอร์จำนวนมาก ที่ต้องการใช้งานอินเทอร์เน็ตความเร็วสูงพร้อมๆกัน

การใช้งาน DSL Router ต้องทำงานร่วมกับ DSL Modem ในด้านการทำงานแล้ว DSL Router จะทำหน้าที่เป็น DHCP Server คอยจ่ายหมายเลขไอพี แอดเดรส (IP Address) ให้กับเครื่องลูกข่าย[7] และจะคอยรับการร้องขอเพื่อเชื่อมต่ออินเทอร์เน็ตจากเครื่องลูกข่าย แล้วจะคอยส่งคำสั่งไปหมุน Modem DSL เพื่อเชื่อมต่อไปยัง ISP นอกจากนี้ DSL Router ยังคอยทำหน้าที่ค้นหาเส้นทางในเครือข่ายอินเทอร์เน็ต และเป็นตัวเชื่อมต่อเครือข่ายอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์อีกด้วย

การใช้งานอินเทอร์เน็ตความเร็วสูงผ่านเทคโนโลยี DSL จะใช้คู่สายโทรศัพท์ทั่วๆไปที่มีหมายเลขติดตั้งไว้ตามบ้าน และในสำนักงานเป็นเส้นทางสื่อสารข้อมูลระหว่างผู้ใช้งานกับผู้ให้บริการอินเทอร์เน็ต โดยคู่สายโทรศัพท์ดังกล่าวเป็นสายสัญญาณที่เชื่อมจากชุมสายโทรศัพท์ในแต่ละพื้นที่ของผู้ให้บริการโครงข่ายโทรศัพท์พื้นฐาน

---

[7] ในกรณีที่ระบบอินเทอร์เน็ต DSL ทำการเชื่อมต่อเครื่องลูกข่าย การใช้สายสัญญาณที่เชื่อมต่อเครื่องลูกข่ายกับอุปกรณ์ DSL Router มักจะใช้สายโคแอ็กเชียล (Coaxial Cable) โดยในสายโคแอ็กเชียลจะมีลวดโลหะนำไฟฟ้าอยู่ภายในแค่เส้นเดียว ซึ่งปกติจะใช้ทองแดงมีฉนวนหุ้มอยู่ 2 ชั้นและมีโลหะที่นำมาถักกันเป็นแพอยู่ตรงกลางระหว่างฉนวนส่วนชั้นนอกจะมีพลาสติกหุ้มอยู่อีกชั้นหนึ่ง สำหรับการทำงานสายโคแอ็กเชียล จะสามารถส่งสัญญาณที่มีช่วงของความถี่ได้กว้างกว่าสายคู่ตีเกลียว สำหรับสายไฟเบอร์ออปติกหรือสายใยแก้วนำแสง จะทำมาจากท่อแก้วหรือพลาสติกโดยจะส่งสัญญาณในรูปของแสง มักใช้เป็นสายนำสัญญาณของระบบเครือข่ายหลัก (Backbone) (อ้างใน จักกริช พฤษการ, การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Communication and Networking), หน้า 125 และ หน้า132)

2.1.1.3 บริการอินเทอร์เน็ตที่ใช้เคเบิ้ล Modem (Cable Modem)

บริการอินเทอร์เน็ตประเภทนี้เป็นเทคโนโลยีที่ค่อนข้างเก่าที่มาพร้อมกับระบบเคเบิ้ลทีวี ซึ่งสายเคเบิ้ลทีวีที่ใช้จะมีแบนด์วิธกว้างถึง 750 เมกะเฮิรตซ์ และย่านความถี่ที่ผู้ให้บริการเตรียมไว้รอสำหรับเปิดให้บริการอินเทอร์เน็ตความเร็วสูงอยู่แล้ว เพียงแค่ติดต่อบริษัทผู้ให้บริการเคเบิ้ลทีวีก็จะได้ Modem มาต่อกับสายเคเบิ้ลนี้ก็จะใช้งานได้

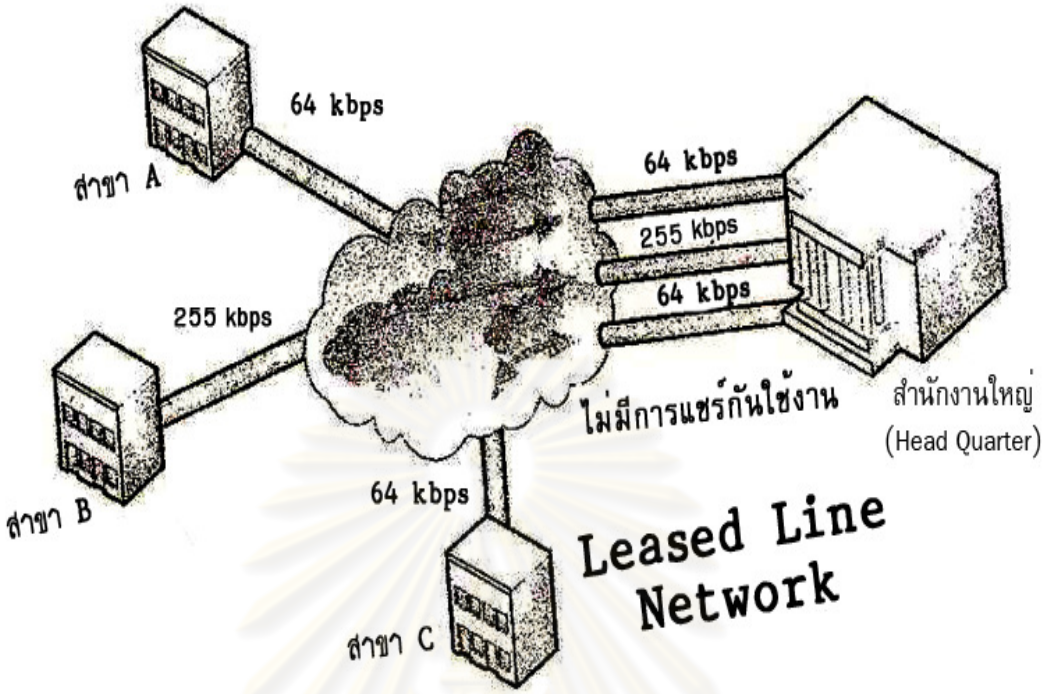
ในด้านเทคโนโลยีแล้ว Cable Modem นั้นเหมาะสำหรับครัวเรือนที่มีเคเบิ้ลทีวี โดยใช้สายโคแอ็กเชียล (Coaxial Cable) เป็นสื่อกลาง การใช้งานก็เพียงแต่ต่อสายเคเบิ้ลออกมาจากกล่องเชื่อมสัญญาณ (Set Top Box) และต่อเข้ากับคอมพิวเตอร์ก็สามารถใช้งานได้ ทางด้านความเร็วแล้ว Cable Modem จะมีความเร็วดาวน์โหลด 27 เมกะบิตต่อวินาที และอัพโหลดที่ 2.5 เมกะบิตต่อวินาที แต่สายสัญญาณเส้นนี้ใช้งานร่วมกันหลายๆ บ้านจึงต้องแชร์กันใช้งาน นั่นอาจจะเกิดปัญหาการใช้บริการอินเทอร์เน็ตช้าได้ หากมีผู้ใช้หลายๆคนพร้อมกัน

2.1.1.4 บริการอินเทอร์เน็ตผ่านวงจรเช่าความเร็วสูง (Leased Line)

ในธุรกิจธนาคารการเงิน ธุรกิจสื่อสาร หรือธุรกิจอื่นๆที่ต้องเชื่อมต่อระหว่างสาขาต่างๆ เข้าด้วยกันจะใช้บริการอินเทอร์เน็ตในระบบวงจรเช่า (Leased Line) ซึ่งเป็นวงจรเช่าความเร็วสูงนิยมใช้งานในช่วง 64 กิโลบิต ถึง 100 เมกะบิตต่อวินาที เป็นระบบที่มีเสถียรภาพสูง มีความแน่นอนและมีการรับประกันถึงคุณภาพการให้บริการ[8]

---

[8]อรรณพ ขันธิกุลและอำนาจ มีมงคล, ติดตั้งและใช้งาน Hi Speed Internet, หน้า 57-58



ในการทำงานของวงจรเช่าจะเป็นการเชื่อมต่อแบบจุดต่อจุด (Point to Point) ที่ไม่มีการแชร์กันใช้งาน ความเร็วจึงได้เต็มตามที่ขอใช้บริการไป นิยมใช้งานกัน 2 รูปแบบหลักๆคือ

1. ใช้เชื่อมต่อระหว่างสาขา เพราะมีเสถียรภาพดีและปลอดภัยสูงจากการดักฟังข้อมูล

2. ใช้เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เพราะปัจจุบันอินเทอร์เน็ตมีความสำคัญไม่น้อยกว่าระบบโทรศัพท์ หากระบบอินเทอร์เน็ตล่มแล้วก็แทบจะทำงานไม่ได้ การเชื่อมต่อแบบนี้มีประโยชน์มาก สามารถนำมาประยุกต์ใช้งานได้หลายประเภท

การติดตั้ง Leased Line จะต้องเดินสายใหม่เพื่อรับประกันว่าสายจะมีคุณภาพดี ไม่สามารถใช้สายโทรศัพท์ที่มีอยู่ในการรับ-ส่งข้อมูลได้ ซึ่งเจ้าหน้าที่ของฝ่ายผู้ให้บริการจะต้องตรวจสอบว่าชุมสายในบริเวณนี้สามารถให้บริการได้หรือไม่ จากนั้นก็เตรียมอุปกรณ์ทั้ง Modem, เราท์เตอร์ ซึ่งต้องสั่งมาเฉพาะทำให้มีราคาแพง การติดตั้งจะต้องคำนวณความยาวสายว่าลากไปยาวเท่าไร หากเกิน 6,000 ฟุตก็ต้องติดตั้งตัวทวนสัญญาณ

2.1.2 บริการอินเทอร์เน็ตแบบไม่ใช้สายสัญญาณ (Wireless)

ในช่วงหลายปีที่ผ่านมาได้มีการพัฒนาแบบก้าวกระโดดของระบบคอมพิวเตอร์ โดยเฉพาะการพัฒนาทางด้านเน็ทเวิร์ก (Network) ไม่ว่าจะเป็นความเร็วในการสื่อสาร รูปแบบการให้บริการใหม่ๆ ความง่ายในการเชื่อมต่อ (ระบบปฏิบัติการช่วยสนับสนุน) การพัฒนาแบบก้าวกระโดดนี้มีผลสืบเนื่องจากการใช้งานของผู้ใช้มากขึ้น รวมถึงผู้ให้บริการต่างๆ ได้จัดบริการใหม่ๆ ที่รองรับการทำงานบนอินเทอร์เน็ตมากขึ้น สิ่งเหล่านี้จึงเป็นแรงผลักดันให้การพัฒนาทางด้าน Network รวดเร็วมากขึ้นตามไปด้วย

การพัฒนาแบบก้าวกระโดดดังกล่าวนี้ส่งผลให้เกิดเทคโนโลยีระบบเครือข่ายไร้สาย (Wireless LAN) ขึ้น เทคโนโลยีดังกล่าวนี้เป็นเทคโนโลยีที่ใช้ระบบเชื่อมโยงระหว่างคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ที่ใช้สายกับไม่ใช้สายเข้าด้วยกัน หรือเชื่อมต่อกับอินเตอร์เน็ตโดยอาศัยคลื่นวิทยุ (Radio Frequency: RF) รับส่งข้อมูลแทนสายเคเบิ้ล ซึ่งคลื่นวิทยุที่ใช้นั้นอยู่ในย่านความถี่ ISM (Industrial Scientific and Medical) ซึ่งเป็นย่านความถี่สาธารณะสามารถใช้งานโดยไม่ต้องขออนุญาต โดยในแต่ละประเทศมีช่องสัญญาณที่อนุญาตให้ใช้งานต่างกัน สำหรับประเทศไทย กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ออกคู่มือประกอบกฎกระทรวงเรื่องกำหนดให้เครื่องวิทยุคมนาคมและสถานีวิทยุคมนาคมบางประเภทได้รับยกเว้นไม่ต้องได้รับใบอนุญาต พ.ศ. 2547 ซึ่งได้กำหนดให้เครื่องวิทยุคมนาคมที่ใช้งานโดยผ่านเครือข่ายไร้สาย (Wireless LAN) ในย่านความถี่ 2400-2500 MHz (2.4-2.5 GHz) และมีกำลังส่งไม่เกิน 100 mW แบบ E.I.R.P. (equivalent isotropically radiated power) เป็นเครื่องวิทยุคมนาคมที่ได้รับยกเว้นไม่ต้องได้รับใบอนุญาต ทำ มี ใช้ นำเข้า นำออก และค้าซึ่งเครื่องวิทยุคมนาคมและตั้งสถานีวิทยุคมนาคม[9]

---

[9] กฎกระทรวงกำหนดให้เครื่องวิทยุคมนาคมและสถานีวิทยุคมนาคมบางประเภทได้รับยกเว้นไม่ต้องได้รับใบอนุญาต พ.ศ. 2547 อาศัยอำนาจตามความในมาตรา 6 วรรคสอง และมาตรา 11 วรรคสี่ แห่งพระราชบัญญัติวิทยุคมนาคม พ.ศ. 2498 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติวิทยุคมนาคม(ฉบับที่ 3) พ.ศ. 2535 และมาตรา 29 (5) แห่งพระราชบัญญัติวิทยุคมนาคม พ.ศ. 2498 รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารออกกฎกระทรวงไว้ ดังต่อไปนี้

ข้อ 2 เครื่องวิทยุคมนาคมที่มีลักษณะหรือที่ใช้ในกิจการดังต่อไปนี้ ได้รับยกเว้นไม่ต้องได้รับใบอนุญาตทำ มี ใช้ นำเข้า นำออก และค้าซึ่งเครื่องวิทยุคมนาคม

นอกจากนี้ยังมีคำศัพท์ใหม่ๆ ที่เกิดตามมาพร้อมกับระบบเครือข่ายไร้สายด้วย เช่น Wi-Fi, Hot Spot ซึ่ง Wi-Fi นั้นหมายถึงเครื่องหมายการค้าของกลุ่มบริษัทขายอุปกรณ์เครือข่าย ใช้เรียกอุปกรณ์เครือข่ายไร้สายตามมาตรฐาน IEEE 802.11b ถ้าเห็นเครื่องหมาย Wi-Fi ที่อุปกรณ์ใด แสดงว่าอุปกรณ์นั้นเข้ากันได้กับมาตรฐาน IEEE 802.11b ส่วน Hot Spot หมายถึงรูปแบบการให้บริการอินเทอร์เน็ตโดยใช้เทคโนโลยีเครือข่ายไร้สาย ผู้ให้บริการจะติดตั้งอุปกรณ์ที่เรียกว่าอุปกรณ์กระจายสัญญาณไร้สาย (แอกเซสพอยต์ : Access Point) ทำหน้าที่กระจายคลื่นวิทยุไว้ตามแหล่งชุมชน เช่น สนามบิน ศูนย์ประชุม ห้างสรรพสินค้า โรงแรม เพื่อรับและส่งสัญญาณวิทยุจากอุปกรณ์ไร้สาย เช่น โน้ทบุ๊คที่มีการ์ดไร้สายแล้วเชื่อมต่อผ่าน Access Point เข้ากับอินเตอร์เน็ตความเร็วสูง โดยที่ผู้ใช้บริการจะต้องซื้อบริการสำหรับการเชื่อมต่อคล้ายกับการซื้อบริการอินเทอร์เน็ตทั่วไป ในประเทศไทยเริ่มมีสถานที่ให้บริการ Hot Spot แล้ว เช่น Siam Discovery สนามบินดอนเมือง ร้านบ้านไร่กาแฟ ร้านกาแฟ Star Bucks โรงแรมเชอราตัน แกรนด์ลากูน่าภูเก็ต และจะเพิ่มขึ้นอีกหลายแห่งในอนาคต

รูปแบบการจัดเครือข่าย (Topology) ของระบบเครือข่ายไร้สายทางกายภาพ (Physical) เป็นแบบ Star คือมี Access Point เป็นศูนย์กลาง มีเครื่องคอมพิวเตอร์ลูกข่ายอยู่โดยรอบ เชื่อมต่อกับศูนย์กลาง หรือ Access Point โดยตรง ส่วนทางตรรกะ (Logical) เป็นแบบ Bus กล่าวคือใช้ช่องสัญญาณร่วมกันโดยผลัดกันใช้ (Shared media) เมื่อคอมพิวเตอร์เครื่องใดต้องการสื่อสารกับ Access Point การ์ดเครือข่ายไร้สายในเครื่องนั้นจะคอยฟังสัญญาณในระบบเครือข่ายว่า ไม่มีเครื่องใดกำลังสื่อสารกับ Access Point อยู่ จึงจะส่งข้อมูลสื่อสารออกไป การทำงานของ Access Point เทียบได้กับการทำงานของฮับ[10] (Hub) ในเครือข่ายใช้สาย คือเมื่อรับข้อมูลทางคลื่นวิทยุจากคอมพิวเตอร์ต้นทาง Access Point จะส่งข้อมูลต่อไปยังคอมพิวเตอร์ปลายทางซึ่งอาจเป็นคอมพิวเตอร์ในเครือข่ายไร้สายเดียวกันผ่านคลื่นวิทยุ หรือเป็นคอมพิวเตอร์

---

(12) เครื่องวิทยุคมนาคมที่ใช้ความถี่วิทยุ 2400 – 2500 เมกะเฮิรตซ์ กำลังส่งออกอากาศสมมูลแบบไอโซทรอปิก (Equivalent Isotropically Radiated Power : E.I.R.P.) ไม่เกิน 100 มิลลิวัตต์ (สำนักงานคณะกรรมการกฤษฎีกา, [ออนไลน์], 11 สิงหาคม 2553. แหล่งที่มา : http://www.krisdika.go.th)

[10] Hub เป็นสถานที่ของการรวมข้อมูลจากหลาย ๆ ทิศทางและส่งต่อไปยังทิศทางอื่น (อ้างใน widebase.net, “โลกกว้างแห่งเทคโนโลยีสารสนเทศ” [ออนไลน์], 11 สิงหาคม 2553. แหล่งที่มา : http://www.widebase.net/knowledge/itterm/it_term_desc.php?term_id=hub)

ในเครือข่ายใช้สายอีกเครือข่ายหนึ่งผ่านสายเคเบิ้ลที่เชื่อมต่อระหว่างเครือข่ายก็ได้ การสื่อสารระหว่างคอมพิวเตอร์ในเครือข่ายไร้สายไม่สามารถสื่อสารกันโดยตรง ต้องสื่อสารผ่าน Access Point ทำให้เสียเวลา เปลืองแบนด์วิธเนื่องจากการสื่อสาร 1 ครั้ง ต้องส่งข้อมูลผ่านเครือข่ายถึง 2 ครั้ง แต่โดยปกติแล้วการสื่อสารมักเป็นการสื่อสารออกไปยังเครือข่ายใช้สายอื่นมากกว่า เช่น อินเตอร์เน็ตความเร็วสูงหรือเครื่อง Server

ย่านความถี่หนึ่งสำหรับการสื่อสารแบ่งออกเป็นหลายช่องความถี่ Access Point กับคอมพิวเตอร์ในเครือข่ายจะตกลงเลือกใช้ช่องความถี่เดียวกันทั้งเครือข่าย ดังนั้นหากมี Access Point หลายตัวอยู่ในบริเวณใกล้เคียงกัน แต่ละเครือข่ายก็จะมีช่องความถี่ที่ใช้สื่อสารของตัวเองแต่หากมีเครือข่ายมากเกินไป ก็ทำให้สัญญาณรบกวนกันได้ ความเร็วการรับส่งข้อมูลขึ้นกับระยะทางสิ่งรบกวน เช่น อุปกรณ์ไร้สายอื่นที่ใช้คลื่นความถี่ใกล้เคียงกันอย่าง หรือกรณีติดตั้งภายในอาคารมีผนัง กำแพง เสา ฯลฯ อีกทั้ง เมื่อคอมพิวเตอร์เคลื่อนที่ห่างจาก Access Point ความเร็วจะลดลงเป็นลำดับ เช่น จาก 11 เป็น 5.5 เมกะบิทต่อวินาที (Mbps) เมื่อเคลื่อนออกไปไกลกว่านี้ เหลือ 2 หรือ 1 เมกะบิทต่อวินาที (Mbps) หากไกลมากกว่านี้จะรับส่งข้อมูลไม่ได้

สำหรับในส่วนองค์กรที่กำหนดมาตรฐานอุตสาหกรรมอิเล็กทรอนิกส์ หรือ IEEE (Institute of Electrical and Electronic Engineer) ได้กำหนดมาตรฐานเครือข่ายไร้สาย โดยใช้การกำหนดตัวเลข 802.11 แล้วตามด้วยตัวอักษรเช่น 802.11a, 802.11b, 802.11g, 802.11n เป็นต้น ตัวอักษรต่อท้ายจะหมายถึงกลุ่มที่กำหนดมาตรฐานโดยในแต่ละกลุ่มจะทำการพัฒนาขีดความสามารถของระบบให้มีประสิทธิภาพสูงกว่าเดิม

สำหรับบริการอินเทอร์เน็ตแบบไม่ใช้สายสัญญาณ (Wireless) ในที่นี้หมายถึงระบบอินเทอร์เน็ตที่การส่งผ่านข้อมูลบางช่วงไม่ได้ใช้สายสัญญาณเป็นสื่อกลางในการส่งข้อมูลเสมือนหนึ่งอาศัยอากาศที่อยู่รอบๆ ตัวเราทำหน้าที่เป็นสายส่งข้อมูล[11] ซึ่งมีหลากหลายประเภทดังต่อไปนี้

---

[11] จักกริช พฤษการ, การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Communication and Networking), หน้า 133

2.1.2.1 บริการอินเทอร์เน็ตบรอดแบนด์ผ่านดาวเทียม[12]

เป็นเทคโนโลยีผ่านดาวเทียม สำหรับที่ห่างไกลที่สายโทรศัพท์เข้าไม่ถึงหรือไม่มีแม้แต่สัญญาณโทรศัพท์เคลื่อนที่ เพียงแต่น่านฟ้าด้านทิศใต้มีดาวเทียมโคจรอยู่ จากนั้นก็ติดตั้งจานดาวเทียมตัวส่งข้อมูลชี้ไปทางนั้น การรับ/ส่งข้อมูลก็จะอาศัยดาวเทียมไทยคมเป็นตัวทวนสัญญาณส่งข้อมูลไปยังเกตเวย์* สำหรับเชื่อมต่ออินเทอร์เน็ต ที่ตั้งอยู่ ณ ศูนย์โทรคมจังหวัดนนทบุรี

สำหรับการให้บริการอินเทอร์เน็ตบรอดแบนด์ผ่านดาวเทียมที่ผู้ใช้ในบ้านเรารู้จักกันดีก็คือ iPSTAR และ iPTV ซึ่งก็จะมีผู้ให้บริการรายใหญ่อยู่รายเดียวในประเทศไทย คือ โครงการ Broadband Satellite ซึ่งเป็นโครงการจากบริษัท ชินแซทเทลไลท์ จำกัด (มหาชน) สำหรับ iPSTAR จะเป็นรูปแบบการให้บริการอินเทอร์เน็ตความเร็วสูงผ่านดาวเทียมแบบสองทาง โดยการใช้งานทางด้านอินเทอร์เน็ตจะจัดการให้บริการผ่านบริษัท CS Internet ที่เป็นบริษัทในเครือของชินแซทเทลไลท์พร้อมสามารถเปิดให้บริการอินเทอร์เน็ตความเร็วสูงได้ทั่วประเทศ จึงไม่จำกัดในเรื่องของพื้นที่ใช้งาน พร้อมทั้งเป็นการเชื่อมต่ออยู่ตลอดเวลาจึงทำให้สะดวกมากขึ้นเวลาใช้งานซึ่งไม่ต้องมานั่งทำการเชื่อมต่อทุกๆครั้งเมื่อจะใช้งาน ส่วนการให้บริการแบบ iPTV นั้นจะเป็นการให้บริการอินเทอร์เน็ตความเร็วสูงแบบทางเดียวและก็เป็นการให้บริการรูปแบบใหม่ สำหรับการเชื่อมต่ออินเทอร์เน็ตนั้น ผู้ใช้จะสามารถเชื่อมต่อสัญญาณจากดาวเทียมได้โดยตรงด้วยจานรับ

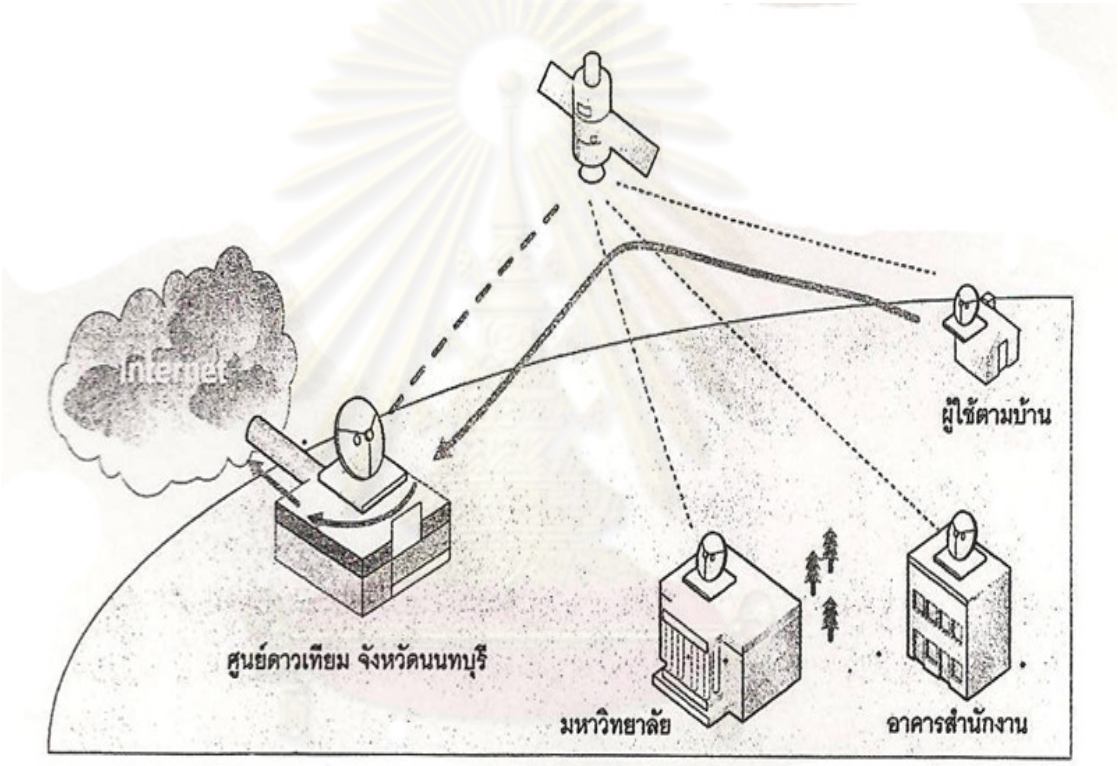
---

[12] อรรณพ ขันธิกุลและอำนาจ มีมงคล, ติดตั้งและใช้งาน Hi Speed Internet, หน้า 21

* เกตเวย์เป็นเสมือนนักแปลภาษาที่ทำให้เครือข่ายที่ใช้โปรโตคอลต่างชนิดกันสามารถสื่อสารกันได้ หากโปรโตคอลที่ใช้รับส่งข้อมูลของเครือข่ายทั้งสองไม่เหมือนกันเกตเวย์ ก็จะทำหน้าที่แปลงโปรโตคอลให้ตรงกับปลายทางและเหมาะสมกับอุปกรณ์ของฮาร์ดแวร์ที่แต่ละเครือข่ายใช้งานอยู่นั้นได้ด้วย (อ้างใน สถาบันนวัตกรรมและพัฒนากระบวนการเรียนรู้, “คอมพิวเตอร์น่ารู้” [ออนไลน์], 10 กันยายน 2552. แหล่งที่มา :

http://www3.ipst.ac.th/research/assets/web/mahidol/computer%2810%29/network/net_wan9.htm)

สัญญาณดาวเทียมที่ติดตั้งอยู่ที่บ้านหรือสถานที่ที่ต้องการใช้งาน ซึ่งจะทำให้ผู้ใช้บริการสามารถรับข้อมูลจำพวกไฟล์ภาพ ไฟล์เสียงหรือไฟล์ข้อมูลขนาดใหญ่ ผ่านระบบเครือข่ายได้รวดเร็วมากยิ่งขึ้น ด้วยความเร็ว 256 Kbps พร้อมบริการ TV ผ่านอินเทอร์เน็ตหรือแม้แต่ TV Reply การรับชมรายการทีวีย้อนหลัง พร้อมบริการอื่นๆ อีกมากมาย ซึ่งการให้บริการอินเทอร์เน็ต หรือบริการรูปแบบอื่นๆ ผ่านดาวเทียมนั้นจะมีราคาทั้งค่าอุปกรณ์ค่าติดตั้งและค่าใช้บริการที่ค่อนข้างสูงมากทีเดียว



2.1.2.2 บริการอินเทอร์เน็ตโดยใช้เทคโนโลยีบรอดแบนด์ของมือถือ (EDGE/CDMA)

เป็นเทคโนโลยีที่ใช้คลื่นโทรศัพท์เคลื่อนที่มาประยุกต์ใช้งานเป็นอินเทอร์เน็ตความเร็วสูงโดยความเร็วในทางทฤษฎีของ EDGE[13] อยู่ที่ 240 กิโลบิตต่อวินาที แต่เปิดให้ใช้งานจริง

[13]เอดจ์ (Enhanced Data rates for GSM Evolution: EDGE) เป็นระบบอินเทอร์เน็ตไร้สาย 2.75G ในเครือข่ายโทรศัพท์มือถือ เป็นเทคโนโลยีตามมาตรฐานสากลที่กำหนดโดย ITU (International Telecommunications Union) คล้ายกับระบบจีพีอาร์เอส แต่มีความเร็วที่สูงกว่า

ประมาณ 100 กิโลบิตต่อวินาที ส่วนของ CDMA[14] นั้นสามารถใช้งานได้สูงถึง 153 กิโลบิตต่อวินาที ทั้งสองเทคโนโลยีนี้จำเป็นจะต้องใช้เครื่องลูกข่ายที่รองรับด้วย

ทางด้านค่าบริการจะมีการคิดทั้งแบบเป็นนาที หรือตามปริมาณข้อมูลที่ผ่านเข้าออก

2.1.2.3 บริการอินเทอร์เน็ต Wimax

WiMAX หรือ Worldwide Interoperability for Microwave Access เป็นมาตรฐานของเทคโนโลยีสำหรับการติดต่อสื่อสารระยะไกล ซึ่งได้กำหนดให้อยู่ในมาตรฐาน IEEE 802.16 ที่เกี่ยวข้องกับเครือข่ายไร้สายแบบบรอดแบนด์ เป็นเครือข่ายไร้สายระดับเมือง ที่มีพื้นที่สัญญาณครอบคลุมในระยะไกลในพื้นที่หรือเขตเมืองเดียวกัน WiMAX เป็นเทคโนโลยีที่เชื่อมต่อในลักษณะที่เรียกว่า “Last Mile” ซึ่งหมายถึง การเชื่อมต่อระหว่างผู้ใช้กับผู้ให้บริการในระยะสุดท้าย

คือที่ประมาณ 200-300 Kbps ซึ่งสูงกว่าจีพีอาร์เอสสี่เท่า (อ้างใน : วิกิพีเดีย สารานุกรมเสรี, “เอดจ์ (เครือข่ายไร้สาย)” [ออนไลน์], 12 ตุลาคม 2553. แหล่งที่มา :

http://th.wikipedia.org/wiki/%E0%B9%80%E0%B8%AD%E0%B8%94%E0%B8%88%E0%B9%8C_%28%E0%B9%80%E0%B8%84%E0%B8%A3%E0%B8%B7%E0%B8%AD%E0%B8%82%E0%B9%88%E0%B8%B2%E0%B8%A2%E0%B9%84%E0%B8%A3%E0%B9%89%E0%B8%AA%E0%B8%B2%E0%B8%A2%29)

[14] Code Division Multiple Access หรือ CDMA คือ เทคโนโลยีการสื่อสารไร้สายด้วยระบบดิจิทัล ซึ่งได้รับการคิดค้นและพัฒนาโดยบริษัท ควอลคอมม์ ซึ่งระบบซีดีเอ็มเอ จะทำหน้าที่แปลงคำพูดเป็นข้อมูลแบบดิจิทัล และส่งผ่านข้อมูลในรูปของสัญญาณวิทยุไปบนเครือข่ายไร้สาย เนื่องจากระบบซีดีเอ็มเอ มีการใช้รหัสที่มีลักษณะเฉพาะในการระบุการโทรแต่ละครั้ง จึงสามารถรองรับผู้ใช้โทรศัพท์จำนวนมากในเวลาเดียวกัน โดยไม่เกิดปัญหาสัญญาณหลุด สัญญาณรบกวน หรือคลื่นแทรก

(อ้างใน ณัฐวุฒิ ทรัพย์บุญมี, “CDMA คืออะไร” [ออนไลน์], 12 ตุลาคม 2553. แหล่งที่มา : http://pirun.kps.ku.ac.th/~b4928057/1.html)

การเชื่อมต่อของ WiMAX นั้นจะคล้ายกับเทคโนโลยี DSL ที่ใช้ผ่านเครือข่ายไร้สาย ที่ความเร็วและขนาดช่วงของสัญญาณจะแปรผันตามระยะทาง โดยตามมาตรฐานแล้ว WiMAX จะรองรับได้ถึง 70 Mbps ในระยะทางที่ไกลถึง 112 กิโลเมตร แต่ในความเป็นจริงแล้วมีปัจจัยหลายอย่างที่รบกวนสัญญาณ โดยเฉพาะอย่างยิ่งการใช้งาน WiMAX ภายในเขตเมืองที่สภาพแวดล้อมต่างๆ รบกวนสัญญาณได้เป็นอย่างดี ทั้งตึกสูง สภาพอากาศ หรือคลื่นสัญญาณอื่นๆ ซึ่งปัจจัยทั้งหมดส่งผลกระทบต่อช่วงความเร็วที่ WiMAX จะรองรับได้ โดยภายในระยะทาง 2 กิโลเมตร WiMAX จะรองรับการขนส่งข้อมูลที่ความเร็ว 10 เมกะบิทต่อวินาที (Mbps) นอกจากข้อจำกัดที่กล่าวมาแล้ว จำนวนผู้ใช้ก็เป็นอีกตัวแปรหนึ่งที่ส่งผลให้ความเร็วที่มีอยู่เพียง 10 เมกะบิทต่อวินาที (Mbps) ลดลงได้อีก เนื่องจากความเร็วในการขนส่งข้อมูลใน WiMAX นี้จะเป็นความเร็วที่แบ่งปันให้กับผู้ใช้ทุกคนภายในเครือข่ายเท่าๆกัน ยิ่งมีผู้ใช้จำนวนมากความเร็วในการขนส่งข้อมูลเฉลี่ยต่อผู้ใช้หนึ่งคนก็จะลดลง

ในส่วนของการส่งข้อมูลมีลักษณะเป็น Full-Duplex คือ สามารถรับส่งข้อมูลได้พร้อมกัน โดยใช้คลื่นวิทยุส่งข้อมูลด้วยความถี่สูงมากและคุณสมบัติที่สำคัญ คือ คลื่นเดินทางเป็นเส้นตรงและคลื่นจะถูกน้ำดูดกลืน (Absorb) ง่าย ซึ่งเป็นปัญหาสำคัญของคลื่นความถี่สูง เนื่องจากสภาวะอากาศที่มีฝนและหิมะตกจะเป็นอุปสรรคสำคัญในการรับส่งข้อมูล

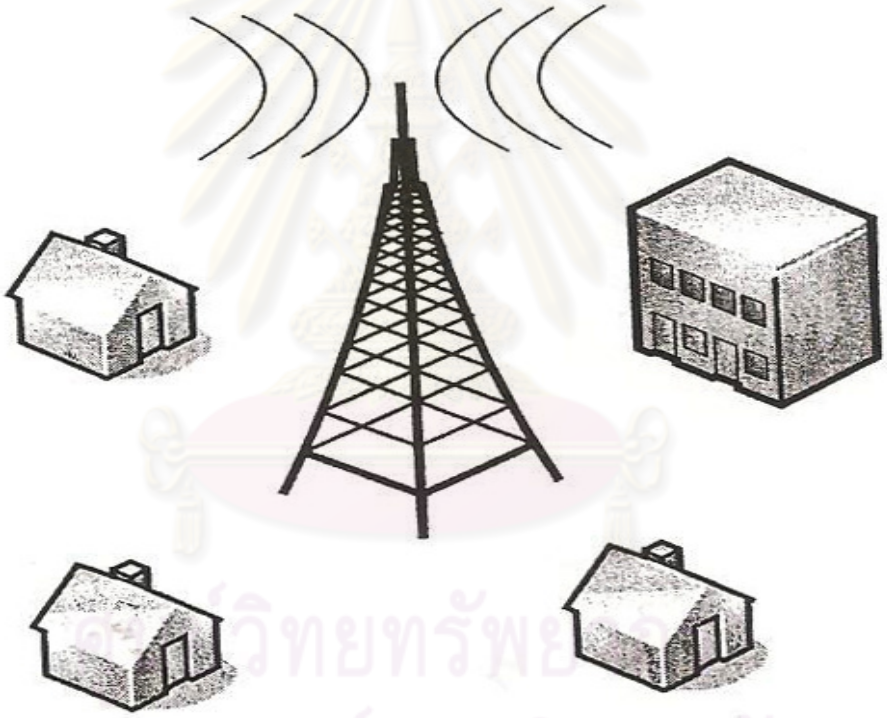
องค์ประกอบและลักษณะของ WiMAX ที่สำคัญมี 2 ส่วน[15] ส่วนแรก คือ กลุ่มของ Base Station (สถานีฐาน) ซึ่งเป็นเสาอากาศที่มีจานรับส่งสัญญาณหลายตัว โดยแต่ละตัวจะดูแลเฉพาะจานรับสัญญาณของตนเท่านั้น ส่วนที่สอง คือ เสาอากาศที่มีจานรับส่งสัญญาณตามบ้านเรือน เรียกการส่งข้อมูลจาก Base Station ไปยังบ้านเรือนว่า Downstream ซึ่งใช้ Base Station ในการควบคุมการรับส่งข้อมูล ส่วนการส่งข้อมูลจากบ้านเรือนไปยัง Base Station เรียกว่า Upstream

ในปัจจุบันได้มีการนำเอาระบบ WiMAX ไปลองใช้งานจริง ในส่วนโครงสร้างหลักได้มีการตั้งเสาสัญญาณ WiMAX กระจายเป็นเครือข่ายครอบคลุมบริเวณที่ต้องการให้บริการหรือนำเอามาใช้เพื่อเพิ่มระยะทางในการให้บริการให้ไกลขึ้นถึงชานเมืองหรือตั้งเสา WiMAX เพื่อรับส่งข้อมูลและกระจายต่อให้กับผู้ใช้ ADSL,DSL ในพื้นที่ที่ลากสายสัญญาณหลักเข้ามาลำบากกลายเป็น Wireless Broadband นั่นเอง

---

[15] สุธี พงศาสกุลชัยและณรงค์ ล่ำดี, การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์, หน้า 294

ส่วนในด้านผู้ใช้งานทั่วไปจะแบ่งออกเป็น 2 ช่วง โดยช่วงแรกในปี 2005 ที่ผ่านมาได้นำเอาระบบมาให้บริการอินเทอร์เน็ต โดยผ่านอุปกรณ์ที่เรียกว่า Fix Wireless Access อุปกรณ์ตัวนี้จะเป็นตัวรับสัญญาณที่สามารถติดที่ไหนก็ได้ เช่น ข้างตัวบ้านหรือตัวตึก แล้วรับสัญญาณ WiMAX มานำไปกระจายต่อยังเครื่องคอมพิวเตอร์ต่าง ๆ ผ่าน Switch ซึ่งตัวอุปกรณ์จะอยู่กับที่ไม่ได้ขยับไปไหน ดังนั้นในช่วงที่สองหลังจากนี้ จะมีการพัฒนาอุปกรณ์ลูกข่ายให้ใช้งานมาตรฐาน IEEE 802.16e เพื่อให้ใช้งานในขณะที่มีการเคลื่อนที่ และสามารถใช้งานข้ามเสาส่งสัญญาณได้ เช่น ขับรถไปรอบเมืองก็ยังใช้งานได้



2.1.2.4 บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย (Wireless LAN)[16]

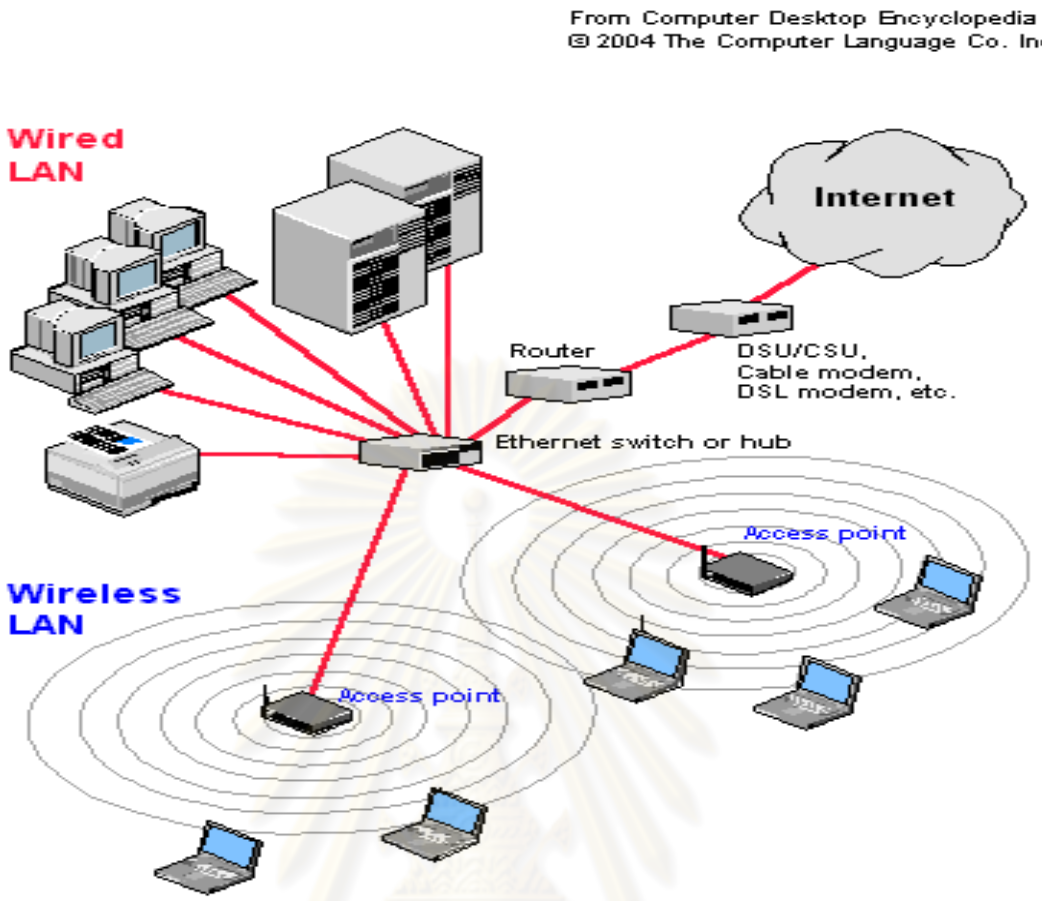
เครือข่ายไร้สาย (Wireless Local Area Network : Wireless LAN) คือ ระบบการสื่อสารข้อมูลที่มีความคล่องตัวมาก ซึ่งอาจจะนำมาใช้ทดแทนหรือเพิ่มต่อกับระบบเครือข่ายใช้สายแบบดั้งเดิม โดยใช้การส่งคลื่นความถี่วิทยุในย่านวิทยุ RF และ คลื่นอินฟราเรด ในการรับและส่งข้อมูลระหว่างคอมพิวเตอร์แต่ละเครื่อง ผ่านอากาศ ทะลุกำแพง เพดานหรือสิ่งก่อสร้างอื่นๆ โดยปราศจากความต้องการของการเดินสาย นอกจากนั้นระบบเครือข่ายไร้สายก็ยังมีคุณสมบัติครอบคลุมทุกอย่างเหมือนกับ ระบบแบบใช้สาย ที่สำคัญก็คือ การที่ระบบเครือข่ายไร้สายไม่ต้องใช้สายทำให้การเคลื่อนย้ายการใช้งานทำได้โดยสะดวก ไม่เหมือนระบบแบบใช้สายที่ต้องใช้เวลาและการลงทุนในการปรับเปลี่ยนตำแหน่งการใช้งานเครื่องคอมพิวเตอร์

เครือข่ายไร้สาย (Wireless LAN) จะประกอบด้วยกลุ่มเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่สื่อสารข้อมูลระหว่างกันโดยการแพร่กระจายคลื่นวิทยุผ่านอากาศรอบตัว การสร้างเครือข่ายไร้สาย (Wireless LAN) ขึ้นมาใช้งานจำเป็นต้องอาศัยอุปกรณ์ที่ออกแบบขึ้นมาใช้งานเฉพาะ

ในการเชื่อมต่อเครือข่ายไร้สาย (Wireless LAN) จำเป็นจะต้องเชื่อมต่อกับเครือข่ายใช้สายด้วย โดยทั่วไปแล้วเครือข่ายใช้สายจะใช้เครือข่ายอีเธอร์เน็ต (Ethernet) ดังปรากฏการติดตั้งอุปกรณ์ต่างๆตามรูปต่อไปนี้

---

[16] อรรณพ ขันธิกุลและอำนาจ มีมงคล, ออกแบบและติดตั้งระบบ Wireless LAN. (นนทบุรี : ไอดีซีฯ, 2547)



ในการทำงานของเครือข่ายไร้สายเพื่อเชื่อมต่อเข้าถึงระบบอินเทอร์เน็ตนั้น จำเป็นจะต้องประกอบไปด้วยอุปกรณ์ต่างๆดังต่อไปนี้

แลนการ์ดไร้สาย (Wireless LAN Card)

อุปกรณ์นี้จะทำให้เครื่องคอมพิวเตอร์ตั้งโต๊ะที่ปกติใช้สายในการเชื่อมต่อสัญญาณกลายเป็นคอมพิวเตอร์ไร้สายที่สามารถสื่อสารข้อมูลถึงกันได้โดยไม่ต้องใช้สายสัญญาณเป็นสื่อกลางเหมือนกับระบบอีเธอร์เน็ตแลน (Ethernet LAN) หน้าที่หลักของแลนด์การ์ดไร้สายก็คือแปลงข้อมูลดิจิทัลที่ได้จากการประมวลผลของเครื่องคอมพิวเตอร์ให้เป็นคลื่นวิทยุแล้วส่งผ่านสายอากาศ (Antenna) แพร่กระจายออกไป และในทางกลับกันก็จะทำหน้าที่รับเอาคลื่นวิทยุที่แพร่กระจายออกมาจากอุปกรณ์ไร้สายอื่นๆ แปลงกลับเป็นข้อมูลดิจิทัลส่งให้เครื่องคอมพิวเตอร์ประมวลผล แลนการ์ดไร้สายที่ผลิตออกมาจำหน่ายมีหลากหลายรูปแบบตามลักษณะช่องเชื่อมต่อของเครื่องคอมพิวเตอร์ที่มี แต่อย่างไรก็ตามสำหรับโน้ทบุ๊คจะติดตั้งแลนการ์ดไร้สายเป็นที่เรียบร้อยแล้ว

อุปกรณ์เข้าใช้งานเครือข่าย (Wireless Access point)

อุปกรณ์เข้าใช้งานเครือข่าย (Wireless Access Point) เป็นอุปกรณ์สำคัญอีกชิ้นหนึ่งบนเครือข่ายไร้สาย ทำหน้าที่เสมือนฮับ (Hub) เชื่อมเครื่องคอมพิวเตอร์ไร้สายและอุปกรณ์ไร้สายต่างๆเข้าด้วยกันเป็นเครือข่าย อีกทั้งเป็นสะพานเชื่อมต่อเครือข่ายไร้สาย (Wireless LAN) เข้ากับเครือข่ายอีเธอร์เน็ต (เครือข่ายใช้สาย) ทำให้อุปกรณ์บนระบบทั้งสองสามารถสื่อสารข้อมูลถึงกันได้

ลักษณะทางกายภาพของ Wireless Access Point ประกอบด้วยสายอากาศแบบซ่อนไว้ภายในหรือแบบติดตั้งภายนอก สามารถถอดเปลี่ยนเป็นสายอากาศเกนสูงเพื่อเพิ่มกำลังรับ-ส่งคลื่นวิทยุให้ครอบคลุมพื้นที่กว้างไกลมากขึ้น

เราเตอร์ (Wireless Broadband Router)

อุปกรณ์ชิ้นนี้พัฒนาขึ้นมาเพื่อตอบสนองผู้ใช้งานเครือข่ายไร้สาย (Wireless LAN) ที่ต้องการเชื่อมต่อเข้าระบบอินเทอร์เน็ตความเร็วสูงผ่านคู่สายโทรศัพท์ (DSL) หรือเคเบิ้ลทีวี (UBC) Wireless Broadband Router ได้นำเอาเทคโนโลยี Broadband Router ซึ่งมีฟังก์ชั่นการทำงานเป็นตัวค้นหาเส้นทางมาผสมผสานเข้ากับ Wireless Access Point ทำให้ผู้ใช้งานคอมพิวเตอร์ไร้สายสามารถสื่อสารข้อมูลไปยังระบบอินเทอร์เน็ตได้โดยผ่านอุปกรณ์ชิ้นนี้

ในปัจจุบันนี้ Wireless Broadband Router ยังได้นิยมนำมาใช้เป็นอุปกรณ์ในการแจกไอพีแอดเดรสให้แก่คอมพิวเตอร์ลูกข่ายที่เข้ามาเชื่อมต่อกับระบบเครือข่ายไร้สายด้วย ซึ่งส่งผลให้คอมพิวเตอร์ในระบบเครือข่ายไร้สายสามารถใช้งานได้พร้อมๆกัน โดยวิธีการทำงานจะใช้หลักการแปลงค่าไอพีแอดเดรส (NAT : Network Address Translation) โดยจะได้อธิบายต่อไปในหัวข้อ 2.2.3

โมเด็ม (Modem)

การเชื่อมโยงเครื่องคอมพิวเตอร์เข้าถึงเครือข่ายอินเทอร์เน็ต จำเป็นต้องมีอุปกรณ์ Modem ทำหน้าที่เป็นตัวเชื่อมระหว่างเครื่องคอมพิวเตอร์ผ่านคู่สายโทรศัพท์ไปยัง Modem ปลายทางของผู้ให้บริการอินเทอร์เน็ต (ISP) ที่ได้จัดเตรียมไว้สำหรับการสื่อสารข้อมูลในระยะไกล ซึ่ง Modem จะทำหน้าที่แปลงสัญญาณที่เป็นข้อมูลดิจิทัลที่เครื่องคอมพิวเตอร์ประมวลผลออกมาเป็นกระแสไฟฟ้าส่งไปตามสายโทรศัพท์เมื่อถึง Modem ปลายทางของผู้ให้บริการอินเทอร์เน็ต

(ISP) ก็จะดำเนินการแปลงกระแสไฟฟ้านั้นกลับมาเป็นสัญญาณข้อมูลดิจิทัลและเข้าถึงขั้นตอนการประมวลผลของเครื่องคอมพิวเตอร์หรือ Server ของผู้ให้บริการอินเทอร์เน็ต (ISP) ต่อไป

หากกล่าวถึงวิธีการใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย (Wireless LAN) ในกรณีการเชื่อมต่อบริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายที่ไม่ได้ตั้งค่าความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สายไว้ เมื่อผู้ใช้บริการนำอุปกรณ์ไร้สายเข้าไปอยู่ในบริเวณที่ Access Point แพร่กระจายคลื่นวิทยุแล้ว โปรแกรมที่ติดตั้งมากับอุปกรณ์ไร้สายจะสามารถตรวจพบได้ว่าในบริเวณนั้นมีเครือข่ายไร้สายใดบ้างที่กำลังส่งคลื่นสัญญาณไร้สายออกมา ซึ่งเมื่อตรวจพบแล้วก็สามารถที่จะเลือกเครือข่ายไร้สายเครือข่ายใดเครือข่ายหนึ่งเพื่อกดเชื่อมต่อ (Connect) เข้าถึงอินเทอร์เน็ตได้โดยทันทีโดย Access Point จะไม่ทำการตอบกลับมาเพื่อให้ผู้ใช้บริการใส่รหัสผ่านในการเข้าใช้งานเหมือนดังระบบเครือข่ายไร้สายที่ได้ตั้งค่าความปลอดภัยในการเข้าถึงระบบเครือข่ายไร้สายไว้

สำหรับการเชื่อมต่อบริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายที่ได้ตั้งค่าความปลอดภัยในการเข้าถึงระบบเครือข่ายไร้สายไว้ไม่ว่าจะเป็นการป้องกันในรูปแบบของ WEP หรือ WPA หรืออื่นๆ (ซึ่งจะได้กล่าวถึงรายละเอียดต่อไป) ก็มีวิธีในการนำอุปกรณ์ไร้สายเข้าไปอยู่ในบริเวณที่ Access Point แพร่กระจายคลื่นวิทยุเช่นเดียวกับการเชื่อมต่อผ่านเครือข่ายไร้สายที่ไม่มีระบบรักษาความปลอดภัยในการเข้าถึงระบบเครือข่ายไร้สาย ซึ่งอุปกรณ์ไร้สายจะสามารถตรวจสอบพบเครือข่ายไร้สายที่มีการตั้งค่าความปลอดภัยการเขาถึงระบบรักษาความปลอดภัยเอาไว้ โดยที่หากผู้ใช้บริการกดเชื่อมต่อ (Connect) โดยที่ไม่ได้ใส่รหัสผ่าน Access Point ก็จะตอบกลับมาเพื่อยืนยันให้ใส่รหัสผ่านจนกระทั่งเมื่อใส่รหัสผ่านถูกต้องแล้ว เครือข่ายไร้สายโดย Access Point จึงจะอนุญาตให้อุปกรณ์ไร้สายเชื่อมต่อเข้าถึงอินเทอร์เน็ตได้

2.2 **ไอพีแอดเดรส** (IP Address)

คอมพิวเตอร์ที่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเครื่องจะต้องมีหมายเลขประจำตัวที่ต้องไม่ซ้ำกันเพื่อใช้อ้างอิงถึงกันได้เปรียบได้เหมือนกับบ้านเลขที่ โดยบ้านแต่ละหลังจะต้องมีบ้านเลขที่เพื่อประโยชน์ในการติดต่อสื่อสารข้อมูล สำหรับในเครือข่ายโดยทั่วไปจะใช้หมายเลขที่

อ้างอิงเรียกว่าไอพีแอดเดรส[17] (IP Address) การกำหนดหมายเลข IP Address จะต้องเป็นไปตามรูปแบบมาตรฐานตามที่กำหนดเท่านั้น ไม่สามารถกำหนดขึ้นได้ตามใจชอบ

IP Address มีเพื่อความจำเป็นเมื่อต้องการติดต่อหรือใช้บริการจากคอมพิวเตอร์เครื่องใดเครื่องหนึ่งในระบบเครือข่ายจะต้องรู้จัก IP Address ของเครื่องนั้นด้วย คล้ายกับการส่งจดหมายที่จะต้องทราบที่อยู่ของผู้รับ ตัวอย่างเช่น หากคอมพิวเตอร์ A ต้องการส่งไฟล์ข้อมูลไปให้คอมพิวเตอร์ B คอมพิวเตอร์ A จะต้องรู้จักหรือมองเห็นคอมพิวเตอร์ B เสียก่อน โดยการอ้างอิงหมายเลข IP Address ของคอมพิวเตอร์ B ให้ถูกต้อง จากนั้นจึงอาศัยโปรโตคอลเป็นตัวรับส่งข้อมูลระหว่างทั้ง 2 เครื่อง แต่อย่างไรก็ตาม ในทางปฏิบัติจะมีการใช้ตัวอักษรย่อแทนหมายเลข IP Address เรียกว่า โดเมนเนม (Domain Name)

IP Address อยู่ในรูปของเลขฐานสอง ใช้ขนาดของข้อมูล 32 บิต โดยแบ่งเป็น 4 กลุ่ม กลุ่มละ 8 บิต เมื่อใดที่ต้องการเขียนให้คนทั่วไปเข้าใจก็เอาเลขฐานสอง 8 บิต ในแต่ละกลุ่มมาเขียนเป็นเลขฐานสิบแล้วคั่นด้วยเครื่องหมายจุด เช่น 192.168.1.2 เป็นต้น

เมื่อใดก็ตามที่เราเชื่อมต่อระบบอินเทอร์เน็ตกับผู้ให้บริการ ผู้ให้บริการจะจัดสรร IP Address ให้เพื่อใช้ติดต่อกับระบบอินเทอร์เน็ตภายนอกเครือข่าย แต่อย่างไรก็ตาม ภายในเครือข่ายของเราอาจจะมี IP Address ที่สงวนไว้สำหรับเครือข่ายภายใน ซึ่งเป็น IP Address ที่เชื่อมต่อออกสู่ระบบอินเทอร์เน็ตไม่ได้ เว้นแต่จะมีการแปลง IP Address ของเครือข่ายภายในให้เป็น IP Address ที่ใช้สำหรับเชื่อมต่อสู่ระบบอินเทอร์เน็ตภายนอกเสียก่อน ดังนั้นจึงสามารถแบ่ง IP Address ออกได้เป็น 2 ลักษณะ คือ Public IP Address และ Private IP Address

2.2.1 Public IP Address

Public IP Address เป็น IP Address ที่คอมพิวเตอร์ต่างๆใช้ติดต่อสื่อสารกันในระบบอินเทอร์เน็ต ซึ่ง IP Address ในโลกนี้มีค่าได้ตั้งแต่ 0.0.0.0 ถึง 255.255.255.255 คือประมาณสี่พันล้านกว่าหมายเลข และจะมีการแบ่งประเภท IP Address กัน เช่น แบ่งเป็นคลาส[18] (Class) ต่างๆ ได้แก่ Class A, Class B, Class C, Class D และ Class E

---

[17] สมเกียรติ รุ่งเรืองลดา, Internet Sharing สำหรับระบบ LAN ในองค์กรและ Internet Cafe. (กรุงเทพมหานคร : โปรวิชั่น, 2544), หน้า 23-24

[18] ธวัชชัย ชมศิริ, ติดตั้ง/ดูแล ระบบเครือข่ายคอมพิวเตอร์อย่างมืออาชีพ. (กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น, 2549), หน้า 44-46

การแบ่ง IP Address ออกเป็นคลาสต่างๆ นั้น เกิดขึ้นเนื่องจากหน่วยงานระดับโลกที่มีหน้าที่ดูแลเรื่อง IP Address ซึ่งมีชื่อว่า InterNIC (The Internet's Network Information Center) มองว่า หน่วยงานที่มีการเชื่อมต่ออินเทอร์เน็ตนั้นมีขนาดเล็กใหญ่ไม่เท่ากัน หน่วยงานที่ใหญ่ๆ ก็ต้องการ IP Address เป็นจำนวนมาก ส่วนหน่วยงานขนาดกลางและขนาดเล็กก็ต้องการเป็นจำนวนน้อยรองลงมาตามลำดับ

คลาส A คือ IP Address ช่วงตั้งแต่ 0.0.0.0 ถึง 127.255.255.255 IP Address ในคลาส A นี้มีไว้จัดสรรให้กับองค์กรขนาดใหญ่มาก โดยที่แต่ละเครือข่ายที่ใช้ IP Address คลาส A จะสามารถต่อเชื่อมคอมพิวเตอร์ได้ถึง 16.7 ล้านเครื่อง

คลาส B คือ IP Address ช่วงตั้งแต่ 128.0.0.0 ถึง 191.255.255.255 IP Address ในคลาส B นี้มีไว้จัดสรรให้กับองค์กรขนาดกลาง โดยที่แต่ละเครือข่ายที่ใช้ IP Address คลาส B จะสามารถต่อเชื่อมคอมพิวเตอร์ได้ถึง 65,534 เครื่อง

คลาส C คือ IP Address ช่วงตั้งแต่ 192.0.0.0 ถึง 223.255.255.255 IP Address ในคลาส C นี้มีไว้จัดสรรให้กับองค์กรขนาดเล็ก โดยที่แต่ละเครือข่ายที่ใช้ IP Address คลาส C จะสามารถต่อเชื่อมคอมพิวเตอร์ได้ 254 เครื่อง (หน่วยงานต่างๆ ในประเทศไทยส่วนมากมักจะใช้ IP Address คลาสนี้)

คลาส D คือ IP Address ช่วง 224.0.0.0 ถึง 239.255.255.255 IP Address ในคลาส D มีไว้เพื่อใช้ในเครือข่ายมัลติคาสต์[19]

---

[19]มัลติคาสต์ คือ เทคโนโลยีในการส่งข้อมูลบนอินเทอร์เน็ตที่พัฒนาให้แตกต่างออกไปจากการส่งข้อมูลโดยทั่วไปที่จะเป็นการส่งแบบ 1 ต่อ 1 กล่าวคือ มีผู้ส่ง 1 คน และผู้รับ 1 คน หรือที่เราเรียกว่า ยูนิคาสต์ (Unicast) ซึ่งเมื่อจำนวนผู้รับเพิ่มขึ้นมากกว่า 1 จึงจำเป็น ต้องส่งข้อมูลซ้ำตามจำนวนของผู้รับ เช่น เมื่อต้องการส่งภาพ Video Conference ไปให้กลุ่มผู้ใช้งานที่อยู่ห่างออกไปอีก 3 คน จำเป็นต้อง ส่งภาพซ้ำถึง 3 ครั้ง ซึ่งเป็นการสูญเสียเวลาและทรัพยากร รวมทั้งทำให้ข้อมูลในเครือข่ายคับคั่งได้

เทคโนโลยี Multicast เป็นเทคโนโลยีช่วยแก้ปัญหานี้ได้ โดยในการส่งแบบ 1 ต่อ N (N คือจำนวนผู้รับ) ผู้ส่งสามารถส่ง ข้อมูลเพียงครั้งเดียวให้กับผู้รับหลายคนได้ในเวลาเดียวกัน (อ้างใน สำนักคอมพิวเตอร์ มหาวิทยาลัยมหิดล, “เทคโนโลยี Multicast” [ออนไลน์], 11 กันยายน 2552. แหล่งที่มา :

คลาส E คือ IP Address ช่วงตั้งแต่ 240.0.0.0 ถึง 254.255.255.255 IP Address ในคลาส E นี้ไม่ได้นำมาใช้งาน เนื่องจากสำรองไว้เพื่อใช้งานในอนาคต

2.2.2 Private IP Address

Private IP Address บางครั้งถูกเรียกว่า “IP ปลอม” หรือ “IP ภายใน” คือ IP Address ที่สงวนไว้ให้สำหรับองค์กรที่ไม่ได้ต่อเชื่อมกับอินเทอร์เน็ต Private IP Address มี 3 กลุ่ม แยกตามคลาสคือ

10.0.0.0 ถึง 255.255.255.255 (1 ชุด คลาส A)

172.16.0.0 ถึง 172.31.255.255 (16 ชุด คลาส B)

192.168.0.0 ถึง 192.168.255.255 (256 ชุด คลาส C)

ปัจจุบัน Private IP Address มักจะถูกนำมาใช้เป็น IP Address ภายในองค์กร เพื่อให้คอมพิวเตอร์ภายในเครือข่ายขององค์กรสามารถสื่อสารกันได้ และเมื่อใดที่คอมพิวเตอร์ที่ใช้ Private IP Address ต้องการเชื่อมต่อเข้าถึงอินเทอร์เน็ตจะต้องมีกระบวนการที่เรียกว่า NAT (Network Address Translation) เพื่อแปลงค่า Private IP Address เป็น Public IP Address เพื่อให้สามารถส่งข้อมูลติดต่อกับระบบอินเทอร์เน็ตภายในเครือข่ายได้ ซึ่งจะกล่าวในรายละเอียดต่อไป

2.2.3 กระบวนการแปลงค่า IP Address (Network Address Translation (NAT))[20]

จากจำนวนของผู้ใช้อินเทอร์เน็ตตามบ้านเรือนและองค์กรขนาดเล็กได้เพิ่มมากขึ้นเรื่อยๆ ในช่วงต้นๆ ซึ่งผู้ใช้เหล่านี้จะเชื่อมต่อกับอินเทอร์เน็ตโดยผ่านสายโทรศัพท์ นั่นหมายความว่าโดยส่วนใหญ่จะมีการใช้งานในช่วงเวลาหนึ่งเท่านั้น ดังนั้นผู้ให้บริการอินเทอร์เน็ต (ISP) สามารถที่จะใช้วิธีกำหนด IP Address โดยอัตโนมัติให้กับผู้ใช้เหล่านี้ได้ แต่ในทุกวันนี้วิธีการและความต้องการของผู้ใช้ได้เริ่มเปลี่ยนไป เนื่องจากสามารถที่จะเชื่อมต่อโดยใช้เทคโนโลยี DSL หรือเคเบิ้ล Modem ได้ นอกจากนั้นแล้วจำนวนของผู้ใช้ในแต่ละบ้าน หรือองค์กรเริ่มมีมากขึ้นด้วย ซึ่ง

---

http://www.cc.mahidol.ac.th/newsletter/Old/Vol7/content_1.htm)

[20] จักกริช พฤษการ, การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Communication and Networking), หน้า 357-359

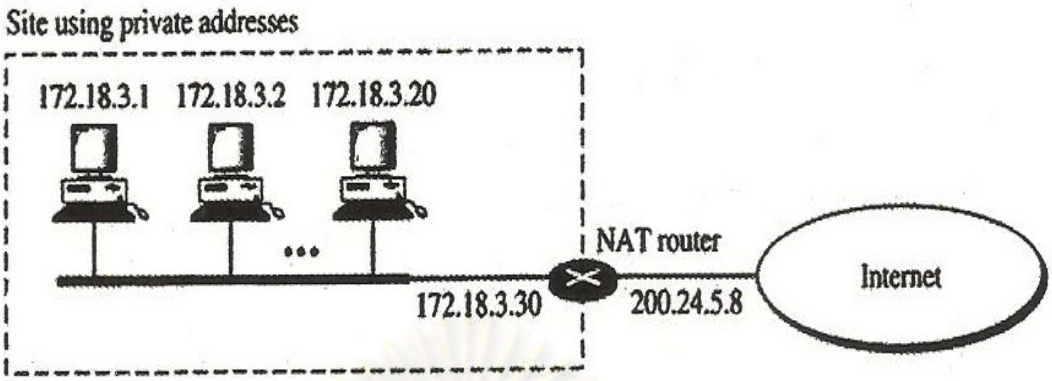
ผู้ใช้บริการเหล่านี้จำเป็นต้องมี IP Address นั่นหมายความว่าอาจจะเกิดปัญหาการขาดแคลน IP Address ได้

อย่างไรก็ตามในปัจจุบันนี้สามารถแก้ปัญหาของการขาดแคลน IP Address ได้โดยใช้วิธีที่เรียกว่า Network Address Translation (NAT) ซึ่งวิธีนี้จะทำให้เครือข่ายภายในตามบ้านเรือนหรือองค์กรมี IP Address เพิ่มขึ้นได้ โดยที่จะใช้ IP Address สำหรับการติดต่ออินเทอร์เน็ตจะมีเพียง 1 IP Address เท่านั้น

เครือข่ายที่อยู่ตามบ้านเรือนหรือองค์กรขนาดเล็กจะเรียกว่า เครือข่ายส่วนตัว (Private Network) ซึ่งเครือข่ายเหล่านี้จะต้องมีไพรเวตไอพีแอดเดรส (Private IP Address) สำหรับกำหนดให้กับผู้ใช้งานแต่ละคน ดังตารางที่ปรากฏข้างล่างนี้จะแสดงให้เห็นถึง IP Address สำหรับเครือข่ายส่วนตัว

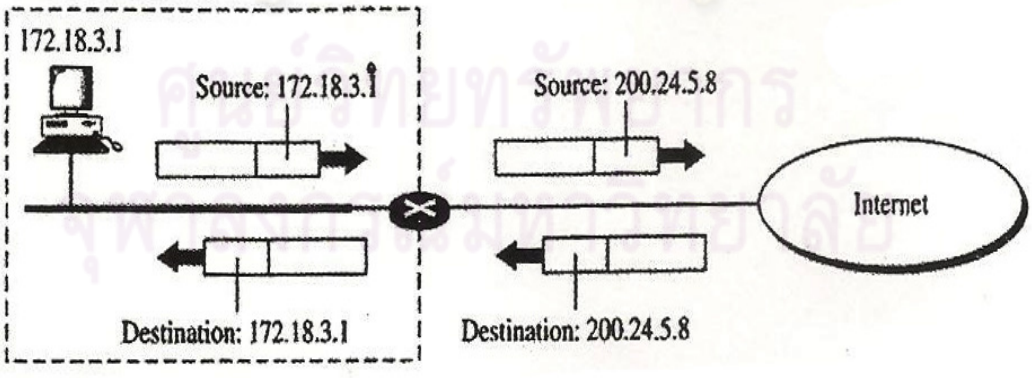
Range			Total
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

จากภาพที่ปรากฏ IP Address เหล่านี้จะถูกสงวนไว้สำหรับการใช้งานตามบ้านเรือนหรือภายในองค์กร ซึ่ง Router จะไม่ส่งข้อมูลจากภายนอกองค์กรไปยังปลายทางที่มี IP Address เหล่านี้ ดังนั้นผู้ใช้ตามบ้านเรือนและองค์กรต่างๆ สามารถที่จะใช้ IP Address เหล่านี้ได้ โดยไม่ต้องขออนุญาตจากผู้ให้บริการอินเทอร์เน็ต แต่ถ้าต้องการที่จะเชื่อมต่อเครือข่ายส่วนตัวกับอินเทอร์เน็ตแล้วจะต้องมี IP Address สำหรับอินเทอร์เน็ตด้วย (Public IP Address) ดังรูปต่อไป ซึ่งจะแสดงถึงตัวอย่างของการเชื่อมต่อเครือข่ายส่วนตัวกับเครือข่ายอินเทอร์เน็ต โดย Router จะต้องมี IP Address 2 IP Address คือ อินเทอร์เน็ตแอดเดรส (Public IP Address) และ Private IP Address นอกจากนั้นแล้วที่Routerจะต้องมีซอฟต์แวร์ NAT ด้วย



จากรูปนี้จะเห็นได้ว่าในเครือข่ายส่วนตัวจะใช้ Private IP Address ส่วน Router จะต้องมีทั้ง Public IP Address และ Private IP Address การเชื่อมต่อแบบนี้อินเทอร์เน็ตจะไม่รู้จักเครือข่ายส่วนตัว แต่จะรู้จักเฉพาะ Router เท่านั้น ดังนั้นถ้าต้องการส่งข้อมูลไปยังเครือข่ายส่วนตัว จะต้องส่งไปที่ IP Address 200.24.5.8 จากนั้นจะเป็นหน้าที่ของ Router ที่จะต้องทำการส่งข้อมูลนั้นให้กับเครือข่ายส่วนตัวต่อไป

สำหรับการแปลง IP Address (Adderss Translation) นั้น ทุกข้อมูลที่ถูกส่งออกไปจากเครือข่ายส่วนตัว จะต้องผ่าน Router โดย Router จะทำการเปลี่ยน IP Address ต้นทาง (Private IP Address) ให้เป็นอินเทอร์เน็ตแอดเดรสหรือ Public IP Address (แอดเดรสของ Router) เสียก่อน ส่วนข้อมูลที่รับเข้ามานั้น Router จะต้องเปลี่ยน IP Address ปลายทาง หรือ Public IP Address (แอดเดรสของ Router) ให้เป็น Private IP Address ดังรูปที่ปรากฏข้างล่างนี้



เมื่อกระบวนการ NAT เริ่มทำงาน จะมีการสร้างตารางภายในซึ่งมีไว้สำหรับบรรจุข้อมูล Private IP address ของเครื่องในเครือข่ายส่วนตัวที่ส่งข้อมูลผ่านกระบวนการ NAT และหลังจากมีการส่งข้อมูลจากเครือข่ายส่วนตัวออกสู่เครือข่ายภายนอก ซอฟแวร์ NAT ก็จะทำหน้าที่

เก็บข้อมูล Private I IP Address ของเครือข่ายส่วนตัวไว้ใน Log File ทำให้ทราบได้ว่า Private IP Address ใดบ้างที่ได้เข้าใช้งานอินเทอร์เน็ต

แต่อย่างไรก็ตาม กระบวนการ NAT ก็มีข้อเสีย[21] เพราะเป็นระบบที่ทำให้ยากต่อการติดตามที่มาของ IP Address หรือผู้ใช้งานอินเทอร์เน็ต เนื่องจากผู้ที่ติดต่อเข้ามาแม้จะใช้ IP Address ที่ถูกต้อง แต่เนื่องจากเป็นการติดต่อเข้ามาโดยผ่านการแปลง IP Address โดยกระบวนการ NAT จึงไม่สามารถติดตามได้ว่า เป็นการติดต่อมาจากเครื่องใดอย่างแท้จริง ทั้งนี้เป็นเพราะคอมพิวเตอร์ทุกเครื่องภายในเครือข่ายส่วนตัวเมื่อสื่อสารผ่านกระบวนการ NAT จะมีการใช้ IP Address ที่ถูกต้องตัวเดียวกันนั่นเอง

และข้อเสียอีกประการหนึ่ง คือ เส้นทางการสื่อสารกับเครือข่ายภายนอก อย่างเช่นอินเทอร์เน็ตจะต้องเกิดช่วงหน่วงเวลา หรือที่เรียกว่า Delay เนื่องจากทุกๆ Private IP Address ภายในเครือข่ายส่วนตัวจะต้องได้รับการแปลงให้เป็น Public IP Address อย่างถูกต้องเสียก่อน ดังนั้น หากมีการติดต่อกับอินเทอร์เน็ตทีเดียวพร้อมๆกัน หลายๆเครื่อง ก็อาจเกิดปัญหาติดขัดได้แม้จะไม่มากนักก็ตาม

---

[21] วิรินทร์ เมฆประดิษฐสิน, “รอบรู้ระบบการทำงานของ NAT ตอนเชื่อมต่ออินเทอร์เน็ตอย่างปลอดภัยและประหยัด” [ออนไลน์], 14 ธันวาคม 2553. แหล่งที่มา : http://www.paktho.ac.th/computerptk/introcom/nat.htm

บทที่ 3
การลักลอบใช้บริการอินเทอร์เน็ตโดยมิชอบและการบังคับใช้กฎหมายของประเทศไทย

ทุกวันนี้คอมพิวเตอร์ได้เข้าไปมีบทบาทในชีวิตมนุษย์มากขึ้นทุกวัน โดยเฉพาะในยุคแห่งข้อมูลข่าวสารอย่างเช่นในปัจจุบัน ซึ่งจะเห็นได้ว่ามีพัฒนาการทางเทคโนโลยีใหม่ๆเกิดขึ้นอย่างรวดเร็ว รวมทั้งพัฒนาการเทคโนโลยีสารสนเทศด้วย แต่ถึงแม้ว่าพัฒนาการทางเทคโนโลยีสารสนเทศนั้นจะถูกนำมาประยุกต์ใช้และก่อให้เกิดประโยชน์มากมายก็ตาม แต่หากนำไปใช้ในทางที่มิชอบแล้วก็อาจก่อให้เกิดความเสียหายอย่างร้ายแรง ทั้งทางเศรษฐกิจและสังคมได้

ดังนั้นด้วยเหตุปัจจัยดังกล่าว จึงก่อให้เกิดรูปแบบใหม่ของอาชญากรรมที่เกิดจากการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดขึ้น ที่เรียกว่าอาชญากรรมทางคอมพิวเตอร์ (Computer Crime Law) ซึ่งสมควรที่จะต้องมีบทบัญญัติของกฎหมายในการลงโทษผู้กระทำความผิด แม้โดยทั่วไปแล้ว กฎหมายอาญาได้ถูกบัญญัติขึ้นมาเพื่อดำเนินการกับการกระทำที่เป็นปฏิปักษ์ต่อสังคม กฎหมายมักจะเพ่งเล็งต่อการกระทำต่างๆ เช่น การลักทรัพย์ การกระทำความเสียหายต่อทรัพย์สินและการกระทำความเสียหายต่อบุคคล โดยปกติกฎหมายมักจะไม่ได้บัญญัติความผิดเฉพาะในส่วนของเหยื่อในการกระทำผิดทางอาญา ไม่มีกฎหมายที่มีเนื้อหามุ่งไปยังเฉพาะส่วนที่เกี่ยวข้องกับเครื่องมือที่ใช้ในการกระทำความผิด[1]

อาชญากรรมคอมพิวเตอร์ เป็นอาชญากรรมที่มีลักษณะเป็นการกระทำการใด ๆ เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหายและผู้กระทำได้รับผลประโยชน์ตอบแทนหรือเป็นการกระทำผิดกฎหมายใด ๆ ซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือและในการ

---

[1]วีระพงษ์ บุญโญภาส, อาชญากรรมทางเศรษฐกิจ (กรุงเทพมหานคร : สำนักพิมพ์นิติธรรม, 2552), หน้า 166

สืบสวนสอบสวนของเจ้าหน้าที่เพื่อนำผู้กระทำผิดมาดำเนินคดีต้องใช้ความรู้ทางเทคโนโลยีเช่นเดียวกัน[2]

ขอบเขตและลักษณะของอาชญากรรมคอมพิวเตอร์นั้นอาจแบ่งออกได้เป็น 3 ประเภท ตามวัตถุหรือระบบที่ถูกกระทำ คือ

- การกระทำต่อคอมพิวเตอร์ (Computer System)
- การกระทำต่อระบบข้อมูล (Information System)
- การกระทำต่อระบบเครือข่ายซึ่งใช้ในการติดต่อสื่อสาร (Computer Network)

หากพิจารณาเป้าหมายของอาชญากรรมคอมพิวเตอร์พบว่ามีเป้าหมายหลายระดับ[3] ดังต่อไปนี้

1.ทำกับชิ้นส่วนของเครื่องคอมพิวเตอร์ เช่น ขโมย Ram ขโมย Hard Disk หรืออุปกรณ์คอมพิวเตอร์อื่นๆ โดยอาจจะเป็นการขโมยอุปกรณ์ต่างๆข้างต้นจากหน่วยงานของรัฐแล้วเอาอุปกรณ์ที่ทำหน้าที่เช่นเดียวกันมาใส่แทน

2.ใช้อุปกรณ์คอมพิวเตอร์ในการกระทำความผิด เช่น ใช้คอมพิวเตอร์ในการเก็บบัญชีลูกค้ายาเสพติด หรือใช้คอมพิวเตอร์ในการหมิ่นประมาทบุคคลอื่น เป็นต้น

3.สร้างไวรัสคอมพิวเตอร์ หรือส่งสัญญาณรบกวนระบบคอมพิวเตอร์เพื่อให้ระบบคอมพิวเตอร์ล่มไม่สามารถทำงานได้

---

[2] Adslthailand, “ กฎหมายอาชญากรรมคอมพิวเตอร์” [ออนไลน์], 5 สิงหาคม 2552. แหล่งที่มา : http://www.adslthailand.com/forum/viewtopic.php?t=681

[3] ญาณพล ยั่งยืน, “ อาชญากรรมทางคอมพิวเตอร์” [ออนไลน์], 30 เมษายน 2554. แหล่งที่มา : http://elib.coj.go.th/Article/49_9_8.pdf

4.การกระทำแบบใช้ระบบเครือข่ายคอมพิวเตอร์ เช่น การลักลอบโอนเงินหรือเป็นเจ้ามือพนันบนอินเทอร์เน็ตซึ่งมีลักษณะต้องเป็นสมาชิกของเว็บไซต์ดังกล่าวเสียก่อนจึงจะเข้าใช้งานได้

ส่วนมาตรการทางกฎหมายที่ปรากฏอยู่ในกฎหมายต่อต้านอาชญากรรมคอมพิวเตอร์ ของหลายๆ ประเทศพอที่จะสรุปได้ว่ามีการกระทำใน 3 ลักษณะที่กฎหมายได้กำหนดโทษไว้ในฐานความผิดอันเป็นอาชญากรรมคอมพิวเตอร์ ดังต่อไปนี้

(1) การเข้าไปในระบบคอมพิวเตอร์หรือทำการเปลี่ยนแปลงหรือทำให้เสียหายซึ่งระบบคอมพิวเตอร์ ด้วยเจตนากระทำการละเมิดอย่างร้ายแรง เช่น ในกรณีที่ผู้ใดได้เจาะระบบหรือแฮก (hacking) คอมพิวเตอร์ของธนาคาร และเข้าถึงข้อมูลหมายเลขบัตรเครดิต ซึ่งผู้กระทำการดังกล่าวมีเจตนาที่จะใช้ข้อมูลเพื่อการได้มาซึ่งตัวทรัพย์อันมีมูลค่าเป็นเงินถือได้ว่ามีความผิด

(2) การเปลี่ยนแปลงข้อมูลในคอมพิวเตอร์โดยมิได้รับอนุญาต ในกรณีที่ผู้ใดประมาทเลินเล่อไม่ว่าการเปลี่ยนแปลงข้อมูลจะทำให้ข้อมูลเสียหายหรือไม่ก็ตาม บทบัญญัติดังกล่าวนี้มีความมุ่งหมายที่จะให้ครอบคลุมถึงการกระทำผิดในหลายรูปแบบ เช่น การที่นักเจาะระบบ หรือแฮกเกอร์ ได้เจาะเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตและทำให้ข้อมูลในคอมพิวเตอร์เสียหาย

(3) การทำให้เสียหายซึ่งการสื่อสารทางอิเล็กทรอนิกส์ รวมถึงการใช้กลอุบายด้านวิทยาการคอมพิวเตอร์ทำให้การสื่อสารทางอิเล็กทรอนิกส์ขัดข้อง เช่น โดยการโจมตีด้วยการส่งอีเมล์อันไม่พึงประสงค์เป็นจำนวนมากไปยังเว็บไซต์ใดเว็บไซต์หนึ่ง จนเป็นเหตุให้ Server ของระบบดังกล่าวล้มเหลวในการทำงานหรือไม่สามารถให้บริการได้ การกระทำเช่นนี้บางครั้งเรียกว่าการทำให้ระบบปฏิเสธการให้บริการ (Distributed denial of services)

การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายเป็นการกระทำที่กระทบต่อระบบคอมพิวเตอร์ อันมีลักษณะเป็นการเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นเพื่อการแสวงหาประโยชน์ที่มิชอบ ซึ่งแบ่งออกเป็น การลักลอบเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจเพื่อใช้บริการอินเทอร์เน็ตและการลักลอบใช้บริการอินเทอร์เน็ตของผู้อื่นโดยมีวัตถุประสงค์เพื่อกระทำความผิด จึงอาจถือได้ว่าการกระทำดังกล่าวเป็นอาชญากรรมคอมพิวเตอร์รูปแบบหนึ่ง ดังนั้น ก่อนที่จะกล่าวถึงลักษณะของการกระทำความผิดข้างต้น จะต้องพิจารณาลักษณะและความหมายของระบบคอมพิวเตอร์, ระบบข้อมูลและระบบเครือข่ายเสียก่อน

1. ลักษณะและความหมายของคำว่า “ระบบคอมพิวเตอร์”

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้นิยามคำว่า “ระบบคอมพิวเตอร์” ไว้ในมาตรา 3 ว่า

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ซึ่งอาจแยกองค์ประกอบของความหมายดังกล่าว ได้ดังนี้[4]

1. เป็นอุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันซึ่งก็คืออุปกรณ์ต่างๆของคอมพิวเตอร์ที่เชื่อมเข้าด้วยกัน เช่น จอภาพ คีย์บอร์ด เม้าท์ หรือเคสซีพียู

2. มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลอัตโนมัติ คือการกำหนดชุดคำสั่งให้คอมพิวเตอร์ทำงานเช่น ระบบปฏิบัติการวินโดว์ หรือระบบปฏิบัติการลีนุ๊ก หรือระบบปฏิบัติการแม็ค

จะเห็นได้จากองค์ประกอบข้างต้นว่า คำว่า “ระบบคอมพิวเตอร์” ที่กล่าวถึงในกฎหมายนั้นเป็นการกล่าวอย่างกว้างๆโดยเน้นไปที่ ฮาร์ดแวร์ (Hardware) เป็นหลักมากกว่าโดยเป็น Hardware ที่มี ซอฟแวร์ (Software) อยู่ดังนั้นหากเป็นเครื่องคอมพิวเตอร์ที่ยังไม่มีการลงชุดคำสั่งจึงไม่เป็นคอมพิวเตอร์ในความหมายนี้ และอาจกล่าวได้ว่าระบบคอมพิวเตอร์ในความหมายของกฎหมายคือคอมพิวเตอร์ที่เชื่อมต่อกันนั่นเอง

2. ลักษณะและความหมายของคำว่า “ระบบข้อมูล”

---

[4] พิญดา เลิศกิตติกุล, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550), หน้า 28

“ระบบข้อมูล” หมายถึง กระบวนการประมวลผลด้วยคอมพิวเตอร์หรือระบบคอมพิวเตอร์สำหรับสร้าง ส่ง รับ เก็บรักษาหรือประมวลผลข้อมูลอิเล็กทรอนิกส์

การให้ความหมายของคำว่า “ระบบข้อมูล” ตามความหมายข้างต้น เป็นการให้ความหมายโดยอาศัยความหมายตามพระราชบัญญัติว่าธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และหากพิจารณาความหมายของคำว่า “ข้อมูลอิเล็กทรอนิกส์ ” ในพระราชบัญญัติฉบับเดียวกันนี้ จะเห็นได้ว่าเป็นการที่กฎหมายรับรองข้อความที่อยู่บนสื่ออิเล็กทรอนิกส์ ว่าเท่าเทียมกับข้อความที่อยู่บนกระดาษ และได้ให้ความหมายของคำว่า “ข้อมูลอิเล็กทรอนิกส์ ” ไว้โดยให้หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร ทำให้เห็นได้ว่าในการก่ออาชญากรรมทางคอมพิวเตอร์นั้น การกระทำความผิดโดยการคุกคามหรือก่อความเสียหายให้เกิดขึ้นคงจะไม่ใช่แต่เพียงกับข้อมูลอิเล็กทรอนิกส์ ในความหมายตามพระราชบัญญัติดังกล่าวเท่านั้น เพราะการกระทำความผิดทางคอมพิวเตอร์นั้น อาจเป็นการกระทำต่อ “ข้อมูล” ซึ่งไม่ได้สื่อความหมายถึงเรื่องราวต่างๆทำนองเดียวกับ “ข้อความ” แต่อย่างใด ตัวอย่างเช่น ข้อมูลซึ่งเป็นรหัสผ่าน หรือลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น แต่อย่างไรก็ตาม แม้ “ข้อมูล” จะมีลักษณะหลากหลายแล้วแต่การสร้างและวัตถุประสงค์ในการใช้งาน แต่ “ข้อมูล” ที่กล่าวถึงนี้ต้องมีลักษณะสำคัญประการหนึ่ง คือ ต้องเป็น “ข้อมูลดิจิทัล (digital)” เท่านั้น

“ข้อมูล” อีกรูปแบบหนึ่งซึ่งมีความสำคัญอย่างมากต่อการรวบรวมพยานหลักฐานอันสำคัญยิ่งต่อการสืบสวน สอบสวนในคดีอาญา คือ “ข้อมูลจราจร (traffic data)” ซึ่งเป็นข้อมูลที่บันทึกวงจรการติดตั้งสื่อสารตั้งแต่ต้นทางถึงปลายทาง ทำให้ทราบถึงจำนวนปริมาณข้อมูลที่ส่งผ่านระบบคอมพิวเตอร์ในแต่ละช่วงเวลา สำหรับข้อมูลต้นทางนั้น ได้แก่ หมายเลขโทรศัพท์ เลขที่อยู่ IP Address (Internet Protocol Address) หรือ IP Address ส่วนข้อมูลปลายทางนั้น ได้แก่ เลขที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (e-Mail Address) หรือที่อยู่เว็บไซต์ (URL) ที่ผู้ใช้อินเทอร์เน็ตเข้าไปดูข้อมูล เป็นต้น นอกจากข้อมูลต้นทางหรือปลายทางแล้วยังรวมถึงข้อมูลต่างๆ เกี่ยวกับเวลาที่มีการติดต่อสื่อสาร วันที่ จำนวนตัวเลขของผู้ที่ติดต่อสื่อสารหรือลักษณะของการใช้บริการหรือประเภทของการติดต่อสื่อสาร เช่น ติดต่อในรูปของไปรษณีย์อิเล็กทรอนิกส์ หรือการโอนแฟ้มข้อมูล เป็นต้น

3. ลักษณะและความหมายของคำว่า “ระบบเครือข่าย”

“ระบบเครือข่าย” หมายความถึง การเชื่อมต่อเส้นทางการติดต่อสื่อสารระหว่างคอมพิวเตอร์หรือระบบคอมพิวเตอร์เข้าด้วยกันเป็นทอดๆ ซึ่งอาจเป็นระบบเครือข่ายแบบปิด คือ การให้บริการเชื่อมต่อเฉพาะสมาชิกเท่านั้น หรือระบบเครือข่ายแบบเปิด ซึ่งหมายถึง การเปิดกว้างให้ผู้ใดก็ได้ใช้บริการในการเชื่อมต่อระบบเครือข่ายหรือติดต่อสื่อสาร เช่น อินเทอร์เน็ต เป็นต้น

สำหรับในส่วนของระบบเครือข่ายไร้สาย (WLAN = Wireless Local Area Network) คือ ระบบการสื่อสารข้อมูลที่มีความคล่องตัวมาก ซึ่งอาจจะนำมาใช้ทดแทนหรือเพิ่มต่อกับระบบเครือข่ายใช้สายแบบดั้งเดิม โดยใช้การส่งคลื่นความถี่วิทยุในย่านวิทยุ RF และคลื่นอินฟราเรด ในการรับและส่งข้อมูลระหว่างคอมพิวเตอร์แต่ละเครื่อง ผ่านอากาศ, ทะลุกำแพง, เพดานหรือสิ่งก่อสร้างอื่นๆ โดยปราศจากความต้องการของการเดินสาย นอกจากนั้นระบบเครือข่ายไร้สายก็ยังมีคุณสมบัติครอบคลุมทุกอย่างเหมือนกับระบบแบบใช้สาย[5]

การกระทำความผิดเกี่ยวกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมิชอบมีอยู่ด้วยกันหลายประเภท โดยที่การกระทำความผิดนั้นส่วนใหญ่จะมีลักษณะเกี่ยวข้องเชื่อมโยงซึ่งกันและกัน ซึ่งผลกระทบจากการกระทำความผิดเกี่ยวกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมิชอบนี้ส่งผลให้เกิดความเสียหายต่อผู้มีสิทธิใช้บริการอินเทอร์เน็ตในหลายๆด้าน ทางออกหรือวิธีการแก้ปัญหาอันเป็นที่ยอมรับของสังคมทั่วไปวิธีหนึ่งก็คือ การนำกฎหมายที่มีอยู่มาจัดการกับการกระทำความผิดประเภทนี้ แต่ในทางปฏิบัติ กฎหมายอาญาในประมวลกฎหมายอาญาที่มีอยู่ไม่สามารถที่จะปรับใช้ได้หรือปรับใช้ได้แต่อาจไม่สมบูรณ์นัก ส่วนการเลือกใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาบังคับกับการกระทำความผิดประเภทนี้ก็อาจจะมีปัญหาบ้างพอสมควร เนื่องจากพระราชบัญญัติฉบับดังกล่าวเพิ่งออกมาใช้บังคับได้ไม่นานและอาจจะมีการกระทำความผิดบางประเภทที่ไม่อยู่ภายใต้บังคับของพระราชบัญญัติฉบับนี้ ดังนั้น ก่อนที่จะทำการวิเคราะห์ถึงปัญหา

---

[5]Ford AntiTrust's Blog, “ระบบเครือข่ายไร้สาย (Wireless LAN)” [ออนไลน์], 11 กันยายน 2552. แหล่งที่มา : http://www.thaicyberpoint.com/ford/blog/id/194

ทางกฎหมาย สมควรอย่างยิ่งที่จะต้องกล่าวถึงลักษณะของการกระทำความผิดเกี่ยวกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมิชอบว่ามีรูปแบบวิธีการใดบ้าง

3.1 การกระทำที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตโดยมิชอบ

การกระทำอันเป็นการลักลอบใช้บริการอินเทอร์เน็ตโดยมิชอบ มีลักษณะประการสำคัญที่ผู้ลักลอบจะต้องเข้าถึงเครือข่ายไร้สายของผู้อื่นโดยมิชอบ การเข้าถึงระบบเครือข่ายไร้สายของผู้อื่นโดยมิชอบนี้จะส่งผลให้ผู้ลักลอบสามารถใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยไม่ต้องชำระค่าบริการอินเทอร์เน็ตซึ่งเป็นค่าบริการที่ผู้ลักลอบสมควรต้องเสียหากตนเป็นสมาชิกรับบริการอินเทอร์เน็ต อีกทั้ง การลักลอบเข้าถึงระบบเครือข่ายไร้สายของผู้อื่น ผู้ลักลอบอาจจะไม่ได้เพียงแค่ต้องการได้รับบริการอินเทอร์เน็ตโดยไม่ต้องชำระค่าบริการเท่านั้น แต่ในบางครั้งผู้ลักลอบได้อาศัยเครือข่ายไร้สายของผู้อื่นที่ตนได้เข้าถึงในการกระทำความผิด ซึ่งการกระทำความผิดดังกล่าวนี้จะมีลักษณะดังต่อไปนี้

3.1.1 การลักลอบเข้าถึงระบบโดยมิชอบ

ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นระบบที่อาศัยคลื่นวิทยุในการเชื่อมต่อระหว่างอุปกรณ์ไร้สายด้วยกันเองหรือเชื่อมต่ออุปกรณ์ไร้สายกับเครือข่ายใช้สาย (Wired LAN) โดยส่วนใหญ่ในระบบเครือข่ายไร้สาย (Wireless LAN) จะเป็นการเชื่อมต่อในลักษณะแบบโครงข่าย (Infrastructure) ซึ่งเป็นการเชื่อมต่ออุปกรณ์ไร้สายแต่ละหน่วยเข้ากับอุปกรณ์เข้าใช้งานเครือข่าย (Wireless Access Point) หรือที่เรียกว่า แอกเซสพอยต์ (Access Point) เพื่อเป็นทางผ่านไปสู่ระบบอินเทอร์เน็ตต่อไป เนื่องจากระบบการเชื่อมต่อแบบโครงข่าย (Infrastructure) ในการกระจายคลื่นวิทยุไม่ได้อาศัยสายสัญญาณใดๆ อุปกรณ์ไร้สายแต่ละเครื่องที่อยู่ภายในบริเวณที่ Access Point กระจายคลื่นอยู่ ก็อาจจะทำการเชื่อมต่อกับ Access Point เพื่อเข้าถึงเครือข่ายอินเทอร์เน็ตต่อไปได้

ในระบบเครือข่ายไร้สาย (Wireless LAN) Access Point จะทำการส่งเฟรมบีคอน (Beacon Frame) ออกมาเป็นระยะเพื่อให้อุปกรณ์ไร้สายในเครือข่ายไร้สาย (Wireless LAN : WLAN) ทำการประสานจังหวะกับ Access Point ส่งผลให้การเข้าใช้สื่อเป็นไปอย่างถูกต้องและมีประสิทธิภาพ ซึ่ง Access Point โดยทั่วไปจะทำการตั้งค่าให้ประกาศชื่อของเครือข่าย (Service

Set Identifier : SSID) นี้ออกมาในเฟรมบีคอนด้วย[6] การประกาศชื่อดังกล่าวทำให้การดักฟังเป็นไปได้โดยง่ายเพราะเหตุที่โปรแกรมที่ติดตั้งมากับอุปกรณ์ไร้สายหลายยี่ห้อรวมถึงเครื่องคอมพิวเตอร์ไร้สายที่ติดตั้งระบบปฏิบัติการ Windows XP สามารถใช้โปรแกรม Windows Zero ตรวจจับ SSID ที่ Access Point แพร่ออกมา ทำให้ล่วงรู้ถึงค่า SSID ของ Access Point ที่ให้บริการในพื้นที่นั้นๆ หรือแม้จะไม่ได้ตั้งใจดักฟังเลยแต่หากผู้ต้องการใช้บริการอินเทอร์เน็ตนำอุปกรณ์ไร้สายเข้ามาในบริเวณขอบเขตสัญญาณที่ Access Point แพร่คลื่นวิทยุอยู่ อุปกรณ์ไร้สายก็สามารถได้รับเฟรมบีคอนและรับทราบข้อมูลดังกล่าวได้ การรับรู้ข้อมูลดังกล่าวเป็นการนำมาซึ่งการเข้าใช้ระบบเครือข่ายไร้สาย (Wireless LAN) โดยไม่ได้รับอนุญาตและอาจเป็นช่องทางให้มีการเจาะระบบต่อไป

แม้ว่าระบบเครือข่ายไร้สาย (Wireless LAN) จะสามารถใช้กลไกควบคุมการเชื่อมต่อในการเข้าถึงระบบเครือข่ายไร้สายด้วยชื่อ SSID ได้โดยที่จะต้องเลือกใช้ Access Point ที่สามารถกำหนดให้เครื่องหยุดการแพร่กระจายชื่อ SSID ด้วยการ Disable ฟังก์ชัน SSID Broadcast ซึ่งเมื่อ Access Point หยุดการแพร่กระจายชื่อ SSID แล้ว ผู้ลักลอบก็จะไม่สามารถพบเครือข่ายไร้สายได้และส่งผลให้ไม่สามารถเชื่อมต่อเข้าสู่เครือข่ายไร้สายได้นั่นเอง และอีกประการหนึ่งเนื่องจาก Access Point ถูกกำหนดเป็นค่ามาตรฐาน (Default) มาจากโรงงานผลิต ค่า SSID ก็จะถูกกำหนดเป็นค่ามาตรฐานมาจากผู้ผลิต เช่น Cisco Aironet กำหนดเป็นชื่อ tsunami เป็นต้น เพื่อป้องกันการลักลอบเข้าสู่เครือข่ายไร้สาย เจ้าของ Access Point ก็จะต้องทำการเปลี่ยนชื่อ SSID ที่เป็นค่ามาตรฐานทันทีที่นำ Access Point มาใช้งาน เนื่องด้วยอุปกรณ์ไร้สายที่ต้องการเชื่อมต่อเข้าสู่เครือข่ายไร้สายจะต้องกำหนดชื่อ SSID ของตนเองให้เป็นชื่อเดียวกันกับชื่อ SSID ของ Access Point ที่ให้บริการในพื้นที่นั้นๆ บุคคลภายนอกที่มีอุปกรณ์ไร้สายแต่ไม่ทราบชื่อ SSID ก็จะไม่สามารถเชื่อมต่อเข้าสู่เครือข่ายไร้สายได้ แต่วิธีการดังกล่าวนี้ในระบบความปลอดภัยยังถือว่าอยู่ในระดับต่ำ เป็นเพียงการรักษาความปลอดภัยแบบที่ง่ายที่สุด สามารถคัดกรองได้เพียงผู้ลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายหรือผู้บุกรุกแบบมือใหม่ได้เท่านั้น แต่หากเป็นการเข้าถึงระบบโดยผู้ลักลอบหรือผู้บุกรุกที่ค่อนข้างมีความชำนาญ การรักษาความปลอดภัยใน

---

[6] อนันต์ ผลเพิ่ม, แลนไร้สาย (Wireless LAN) (กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น, 2550), หน้า 126

การเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) จึงต้องเข้มงวดมากขึ้น โดยอาจใช้วิธีการคัดกรองด้วยแม็คแอดเดรส (MAC Address)[7]

แม็คแอดเดรส (MAC Address) เป็นค่าที่ใช้ในการอ้างอิงถึงการ์ดเครือข่ายที่มีลักษณะเป็นหนึ่งเดียวไม่ซ้ำกันเลย (Unique) และถูกกำหนดค่ามาจากผู้ผลิต โดยปกติการ์ดเครือข่ายนี้จะถูกติดตั้งมาพร้อมกับเมนบอร์ดของเครื่องคอมพิวเตอร์แบบไร้สาย ทำให้ถือได้ว่าการ์ดเครือข่ายไร้สายนี้เป็นสมบัติของผู้ใช้คนนั้น และสามารถใช้ค่าแม็คแอดเดรส (MAC Address) ของการ์ดเครือข่ายนี้เพื่อเป็นการพิสูจน์ตัวจริงของผู้ใช้ผู้นั้นได้ การเพิ่มความปลอดภัยกับระบบเครือข่ายไร้สาย (Wireless LAN) สามารถทำได้โดยการนำหมายเลขแม็คแอดเดรส (MAC Address) ของผู้มีสิทธิใช้งานทุกคนนำไปบันทึกที่ตัว Access Point ที่มีความสามารถในการคัดกรอง โดยตั้งค่าให้อนุญาตการเชื่อมต่อให้แก่อุปกรณ์ไร้สายที่มีค่าแม็คแอดเดรส (MAC Address) ตามที่ได้บันทึกไว้เท่านั้น แต่ก็ยังคงเป็นความปลอดภัยในระดับต่ำ เนื่องจากผู้บุกรุกที่มีความชำนาญสามารถทำการดักฟังและหาค่าแม็คแอดเดรส (MAC Address) ที่ได้รับสิทธิในการเข้าใช้งาน จากนั้นก็จะทำการปลอมตัว (Spoofing) ให้เป็นค่าแม็คแอดเดรส (MAC Address) ที่ดักฟังมาได้ เพื่อทำการเชื่อมต่อเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ต่อไป

การตั้งค่ารักษาความปลอดภัยเครือข่ายไร้สายที่มีประสิทธิภาพ[8]มากกว่า 2 วิธีดังกล่าวข้างต้น ยังมีอีกหลายวิธี ดังรายละเอียดต่อไปนี้

---

[7] เรื่องเดียวกัน, หน้า 127.

[8] การตั้งค่ารักษาความปลอดภัยแบบเดิมที่ถือว่าไม่ปลอดภัยเพียงพอในปัจจุบันคือ

1. การระงับการกระจาย SSID (Hide SSID)

2. การกำหนดสิทธิผู้ใช้โดย MAC Address (MAC filtering / Access control)

3. การเข้ารหัสแบบ WEP (Wired Equivalent Privacy)

ซึ่งการตั้งค่ารักษาความปลอดภัยที่ถือว่าปลอดภัยเพียงพอในปัจจุบันมีดังนี้ (การตั้งค่ารักษาความปลอดภัยต่อไปนี้สามารถใช้ร่วมกับข้อ 1-3 ได้เพื่อความปลอดภัยที่เพิ่มขึ้น ยกเว้นข้อ 3 ใช้พร้อมกันกับข้อ A. ไม่ได้)

1. การตั้งค่า WEP[9] (Wired Equivalency Privacy)

เป็นวิธีการที่นิยมใช้กันมาก โดยปกติแล้วการสื่อสารข้อมูลระหว่างอุปกรณ์ไร้สายบนเครือข่ายไร้สายจะอยู่ในรูปของข้อมูลที่ไม่มีการเข้ารหัสหรือเรียกว่า Plain Text Message หรือ Clear Text ทำให้ผู้ลักลอบเข้าถึงเครือข่ายไร้สายสามารถโจรกรรมข้อมูลที่กำลังสื่อสารในเครือข่ายไร้สายได้ ดังนั้น เพื่อป้องกันข้อมูลไม่ให้ถูกดักจับจึงจำเป็นต้องมีการเข้ารหัส โดยนำเอา plain Text Message นั้นมาเข้ารหัสก็จะกลายเป็นข้อมูลที่ถูกเข้ารหัสไว้ (Encrypted Message) ที่จะไม่สามารถอ่านและตีความได้ เมื่อข้อมูลที่ถูกเข้ารหัสไว้ถูกส่งออกไปในอากาศจึงไม่ใช่ข้อมูลที่แท้จริง ผู้ลักลอบก็จะได้รับข้อมูลที่ผิดไปการตั้งค่ารหัส (Key) ใน WEP มีรหัส 2 ชนิด คือ ขนาด 64 บิต หรือ 128 บิต

เมื่อตั้งค่ารหัสใน Access Point แล้วก็สามารถเชื่อมต่อเข้าถึงเครือข่ายไร้สายได้ โดยเมื่อเชื่อมต่อเข้ากับเครือข่ายไร้สายแล้ว Access Point จะตอบกลับมาให้ผู้ใช้งานป้อนค่ารหัส (Key) เมื่อป้อนรหัสผ่านที่ถูกต้องก็จะสามารถใช้งานเครือข่ายไร้สายได้ต่อไป

2. WPA[10] (Wi-Fi Protected Access)

A. การเข้ารหัสตามมาตรฐาน IEEE802.11i (WPA2) (มีรายงานว่าเมื่อไม่นานมานี้สามารถถอดและปลอมแปลงการเข้ารหัสได้แล้ว)

B. การเชื่อมต่อกับระบบกลางของผู้ให้บริการอินเตอร์เน็ต เช่น RADIUS Server ซึ่งจะกำหนดสิทธิทุกอย่างของผู้ใช้งานโดย “ชื่อผู้ใช้และรหัสผ่าน” (Username/Password) ตามมาตรฐาน IEEE802.1x ตัวอย่างการให้บริการประเภทนี้คือ TRUEwifi, TOTwifi, CATwifi เป็นต้น

C. การเชื่อมต่อแบบ VPN (Virtual Private Network) หากต้องการเชื่อมต่อเข้าระบบของบริษัทหรือระบบส่วนตัว เสมือนการสร้างอุโมงค์ลับเพื่อเชื่อมต่อระบบที่ต้องการความปลอดภัยสูง

(สัมภาษณ์ ฤทธิไกร ขัณฑวีระมงคล, ผู้ก่อตั้งเว็บไซต์ http://www.adslthailand.com, 25 ธันวาคม 2553.)

[9] อรรณพ ขันธิกุลและอำนาจ มีมงคล, ออกแบบและติดตั้งระบบ Wireless LAN 2nd edition (นนทบุรี : ไอดีซีฯ, 2553), หน้า 424 – 427

เป็นระบบรักษาความปลอดภัยของเครือข่ายที่ออกแบบมาเพื่อแก้ปัญหาความบกพร่องของระบบรักษาความปลอดภัยแบบ WEP โดยระบบรักษาความปลอดภัยแบบ WPA รองรับการเข้ารหัสกุญแจแบบเปลี่ยนรหัสตลอดเวลาซึ่งจะปลอดภัยมากกว่า สำหรับการเชื่อมต่อเข้ากับเครือข่ายไร้สายที่ตั้งระบบความปลอดภัยโดยใช้ WPA นั้นมีลักษณะเช่นเดียวกันกับเครือข่ายไร้สายที่ตั้งระบบความปลอดภัยโดยใช้ WEP กล่าวคือ เมื่ออุปกรณ์ไร้สายเลือกเชื่อมต่อกับเครือข่ายไร้สายที่ตั้งมาตรการป้องกันเข้าถึงการตั้งค่า WPA Access Point ของเครือข่ายไร้สายจะตอบกลับมาให้ผู้ใช้งานป้อนค่ารหัส (Key) เมื่อป้อนรหัสผ่านที่ถูกต้องก็จะสามารถใช้งานเครือข่ายไร้สายได้ต่อไป

WPA แบ่งเป็นระบบรักษาความปลอดภัยสองประเภท คือ WPA และ WPA2 WPA ได้รับการออกแบบให้ทำงานกับการ์ดเชื่อมต่อเครือข่ายแบบไร้สายแต่อาจไม่สามารถทำงานกับแอกเซสพอยต์หรือ Router รุ่นเก่า การใช้ระบบรักษาความปลอดภัยแบบ WPA2 จะมีความปลอดภัยมากกว่า WPA

3. การพิสูจน์สิทธิการเข้าใช้งานเครือข่ายไร้สายด้วย Radius Server[11]

ระบบเครือข่ายไร้สายที่ตั้งมาตรการป้องกันการเข้าถึงโดยใช้การพิสูจน์สิทธินี้ เมื่อผู้ใช้งานต้องการเข้าใช้งานเครือข่ายไร้สายจะต้องถูกพิสูจน์สิทธิการเข้าใช้งานก่อนโดย Radius Server จะทำหน้าที่เป็นผู้ตรวจสอบและอนุญาตให้เข้าใช้งานเครือข่ายไร้สายได้ ซึ่งใน Radius Server จะบรรจุข้อมูลของผู้มีสิทธิใช้งานและรหัสผ่าน ดังนั้น ผู้ที่จะสามารถใช้งานเครือข่ายไร้สายได้จะต้องมีบัญชีรายชื่ออยู่ในฐานข้อมูลของ Radius Server เท่านั้น การติดตั้งมาตรการป้องกันการเข้าถึงในลักษณะนี้มีความปลอดภัยสูงเหมาะกับองค์กรขนาดใหญ่

---

[10] อนันต์ ผลเพิ่ม, แลนไร้สาย (Wireless LAN), หน้า 138

[11] อรรณพ ขันธิกุลและอำนาจ มีมงคล, ออกแบบและติดตั้งระบบ Wireless LAN 2nd edition, หน้า 447 – 449

4. การสร้างเครือข่ายส่วนตัวแบบเสมือน (Virtual Private Network (VPN))[12]

การตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายวิธีการนี้จะมีลักษณะเป็นการสร้างอุโมงค์หรือท่อขึ้นมาเพื่อใช้เป็นช่องทางที่ปลอดภัยสำหรับการสื่อสารข้อมูลระหว่างอุปกรณ์ไร้สายกับเครือข่ายหลัก โดยเจ้าของเครือข่ายไร้สายจะต้องติดตั้งโปรแกรม VPN Client ลงบนอุปกรณ์ไร้สายของตน โปรแกรมดังกล่าวจะทำหน้าที่สร้างอุโมงค์ผ่าน Access Point ไปยัง VPN Server เพื่อเชื่อมเข้าถึงเครือข่ายหลักอีกที อุโมงค์ที่สร้างขึ้นจะช่วยป้องกันไม่ให้ผู้ลักลอบเข้าถึงเครือข่ายไร้สายดักจับข้อมูลที่กำลังสื่อสารบนเครือข่ายไร้สาย การติดตั้งมาตรการป้องกันการเข้าถึงในลักษณะนี้มีความปลอดภัยสูงเหมาะกับองค์กรขนาดใหญ่เช่นเดียวกับการพิสูจน์สิทธิการเข้าใช้งานเครือข่ายไร้สายด้วย Radius Server

แต่อย่างไรก็ตาม แม้ว่าจะมีการตั้งค่ารักษาความปลอดภัยด้วยวิธีต่างๆที่กล่าวมาแล้ว การที่อุปกรณ์ไร้สายชิ้นหนึ่งๆจะสามารถเชื่อมต่อเพื่อรับ – ส่งข้อมูลกับเครือข่ายไร้สาย (Wireless LAN) ได้ ในบางครั้งผู้ควบคุมระบบ (ผู้ให้บริการ) ได้กำหนดให้ผู้เข้าใช้งานต้องทำการพิสูจน์ว่าผู้ใช้อุปกรณ์ไร้สายชิ้นนั้นเป็นตัวจริงก่อน (Authentication) เพื่อเป็นการป้องกันการเข้าใช้งานของผู้ที่มิได้รับอนุญาต ซึ่งอาจก่อให้เกิดความเสียหายต่อระบบ หลักการทำงานต้องอาศัยกุญแจรหัส (Key) เช่น รหัสผ่าน (Password) ที่ผู้ร้องขอการตรวจสอบส่งมาให้ระบบทำการตรวจถ้ารหัสตรงก็จะถือว่าเป็นผู้ใช้งานที่ถูกต้อง ซึ่งถ้าผู้ลักลอบใช้บริการอินเทอร์เน็ตหรือผู้บุกรุกรู้รหัสหรือทำการคาดเดารหัสได้ถูกต้อง หรือทำการดักข้อมูลเพื่อทราบรหัส ก็สามารถรู้และปลอมตัวมาเป็นผู้ใช้งานที่มีสิทธิ โดยระบบจะไม่เห็นความแตกต่างของการใช้งานและถือเสมือนว่าตัวจริงเป็นผู้ใช้งานเอง

จากลักษณะของการเข้าใช้ระบบเครือข่ายไร้สาย (Wireless LAN) โดยมิชอบ ดังที่กล่าวมาแล้วนั้น ต่อไปก็ควรที่จะพิจารณาถึง ความหมายของคำว่า “เข้าถึง (Access)” เสียก่อน เนื่องจากความหมายของคำว่า “เข้าถึง” นี้มีความจำเป็นอย่างมากในการวิเคราะห์ว่าผู้ลักลอบเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) จะมีความรับผิดทางกฎหมายหรือไม่ เนื่องจากตามประมวลกฎหมายอาญาและพระราชบัญญัติที่มีโทษทางอาญาอื่นๆมิได้ให้คำจำกัดความ คำๆนี้ไว้แต่อย่างใด

---

[12] เรื่องเดียวกัน, หน้า 450 – 452.

การเข้าถึงคอมพิวเตอร์[13]นั้น ลักษณะของการกระทำคือ “การเข้าถึง” อาจเป็นการเข้าถึงสิ่งต่างๆได้แก่ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์

คำว่า “การเข้าถึง” หมายถึง การเข้าไป การสั่ง การสื่อสาร การนำข้อมูลเข้าไปเก็บไว้ การนำข้อมูลออกมา การใช้ประโยชน์ใดๆจากข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งการเข้าถึงนี้อาจหมายถึง การกระทำอันเป็นเหตุให้คอมพิวเตอร์ปฏิบัติหน้าที่ใดๆ แก้ไขเปลี่ยนแปลง หรือลบโปรแกรมหรือข้อมูล ทำซ้ำหรือย้ายโปรแกรม หรือนำข้อมูลไปเก็บไว้ในที่อื่น การใช้โปรแกรมหรือข้อมูลซึ่งนำออกมาจากคอมพิวเตอร์ที่เก็บโปรแกรมหรือข้อมูลนั้นๆ

การเข้าถึง (access)[14] ระบบคอมพิวเตอร์นั้น อาจแยกออกได้เป็น 2 กรณี คือ การเข้าถึงในความหมายอย่างแคบ คือการเข้าไปโดยเทียบเคียงกับลักษณะของการบุกรุกที่เกิดขึ้นในโลกทางกายภาพ กล่าวคือมีการเข้าไป (inside) ในระบบคอมพิวเตอร์ โดยได้มีการล่วงล้ำเข้าไปอย่างแท้จริงโดยเทียบกับการบุกรุกที่มีการเข้าถึงสถานที่นั้น แต่การเข้าถึงระบบคอมพิวเตอร์ในความหมายอย่างกว้างมีแนวคิดที่อ้างอิงกับการทำงานของระบบคอมพิวเตอร์เป็นหลัก โดยมุ่งเน้นไปที่การทำงานของคอมพิวเตอร์ที่เกิดขึ้นโดยเห็นว่าการเข้าถึงนั้นคือการทำให้ระบบคอมพิวเตอร์ทำงาน หากทำให้ระบบคอมพิวเตอร์มีการตอบสนอง (response) กับคำสั่งที่ได้มีการสั่ง (input) นั้น

---

[13] องอาจ เทียนหิรัญ, “อาชญากรรมทางคอมพิวเตอร์ : การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2546), หน้า 80-81

[14] พิญดา เลิศกิตติกุล, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550), หน้า 35-36

มีนักกฎหมายบางท่าน[15]เห็นว่าถ้อยคำว่า “เข้าถึง” ในกฎหมายไทยค่อนข้างที่จะคลุมเครือว่าเป็นการกระทำในขั้นตอนใด เนื่องจากการที่จะลงโทษบุคคลใดความผิดในกฎหมายอาญาจะต้องมีการกระทำที่ชัดเจนพอสมควรโดยไม่คลุมเครือว่าผู้กระทำความผิดมุ่งหวังหรือเจตนาที่จะกระทำความผิด ดังนั้น จึงเห็นว่าจำเป็นที่จะต้องกำหนดขอบเขตของการเข้าถึง คือ การกระทำการอย่างใดอย่างหนึ่งที่มีลักษณะเป็นการตอบสนองกับเครื่องคอมพิวเตอร์เพื่อให้ได้มาซึ่งการใช้ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ คือจะต้องตีความคำว่า “เข้าถึง” อย่างกว้างที่สุด ซึ่งในทางกฎหมายนานาประเทศได้มีการแบ่งการเข้าถึง โดยพิจารณาลักษณะการเข้าถึงเป็นการเข้าถึงทางกายภาพ คือ การเข้าถึงโดยใช้กายภาพตอบสนองผ่านระบบคอมพิวเตอร์เพียงเครื่องเดียวและการเข้าถึงระยะไกลซึ่งเป็นการเข้าถึงโดยผ่านระบบคอมพิวเตอร์สองเครื่องขึ้นไป โดยในชั้นร่างกฎหมายและความเห็นทางวิชาการของนักกฎหมายไทยได้ให้ความเห็นเป็นแนวทางที่ชัดเจนว่า การเข้าถึงนั้นหมายความรวมถึง การเข้าถึงทางกายภาพด้วย กล่าวคือสรุปได้ว่ากฎหมายไทยถือว่าการเข้าถึงทางกายภาพ เป็นการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ด้วย ดังนั้น จึงสมควรที่จะต้องพิจารณาการกระทำทั้งการเข้าถึงในระยะไกลและการเข้าถึงทางกายภาพเพราะมีความแตกต่างกัน

1. **การเข้าถึงระยะไกล** คือ การเข้าถึงโดยเชื่อมต่อระบบระหว่างคอมพิวเตอร์สองเครื่อง การเข้าถึงคอมพิวเตอร์ของผู้กระทำความผิดนั้นเป็นเพียงการตระเตรียมเท่านั้นยังไม่เป็นการกระทำความผิดแต่อย่างใด เมื่อมีการเชื่อมต่อระบบอินเทอร์เน็ตหรือระบบอื่นใดโดยมีการฝ่ามาตรการป้องกันไปยังเครื่องคอมพิวเตอร์เป้าหมายก็เป็นการลงมือกระทำความผิดแล้วและเมื่อปรากฏในหน้าจอของคอมพิวเตอร์อีกเครื่องหนึ่งโดยผู้กระทำความผิดพร้อมที่จะใช้งานคอมพิวเตอร์ของผู้อื่น การกระทำดังกล่าวก็เป็นความผิดสำเร็จแล้ว

2. **การเข้าถึงทางกายภาพ** คือ การเข้าถึงโดยผู้กระทำความผิดได้ใช้ร่างกายของตนเข้าถึงระบบคอมพิวเตอร์ในเครื่องคอมพิวเตอร์เพียงเครื่องเดียว ดังนั้น เมื่อใดก็ตามที่ร่างกายของผู้กระทำมีการกระทำการตอบโต้กับคอมพิวเตอร์จึงเป็นการเข้าถึงแล้ว

---

[15] ชาตรี ส่งสัมพันธ์, “อาชญากรรมคอมพิวเตอร์ : ศึกษาวิเคราะห์การเข้าถึงโดยมิชอบ,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2552), หน้า 35-36

การเข้าถึงทางกายภาพจะมีขอบเขตเพียงใด ในเรื่องนี้มีความเห็นของนักวิชาการต่างประเทศแบ่งแยกออกเป็น 3 แนวทาง

แนวทางที่ 1 เห็นว่า การเข้าถึงทางกายภาพไม่รวมถึงการมองหน้าจอคอมพิวเตอร์หรืออ่านข้อความบนหน้าจอแล้วจดข้อความโดยไม่ได้มีการตอบโต้กับคอมพิวเตอร์

แนวทางที่ 2 เห็นว่า การเข้าถึงทางกายภาพเพียงแค่มองหน้าจอคอมพิวเตอร์ก็เป็นการเข้าถึงทางกายภาพแล้ว

แนวทางที่ 3 เห็นว่า การเข้าถึงทางกายภาพจะต้องเป็นการสัมผัสที่ก่อให้เกิดการทำงานของเครื่องคอมพิวเตอร์ การกระทำดังกล่าวจึงเป็นการ “เข้าถึง” ทางกายภาพ

นักกฎหมายท่านดังกล่าวยังได้พิจารณาต่อไปอีกว่า ในบางครั้งการเข้าถึงอาจพิจารณาที่วัตถุที่กระทำต่อ (Target) โดยเฉพาะอย่างยิ่งระบบคอมพิวเตอร์ ซึ่งการเข้าถึงระบบคอมพิวเตอร์เป็นการกระทำความผิดแล้ว ด้วยเหตุที่ว่าการเข้าถึงระบบคอมพิวเตอร์ทำให้เกิดการเกรงกลัวว่าจะเกิดอันตรายต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ โดยเป็นการกระทำเบื้องต้นที่นำไปสู่การกระทำความผิดในฐานอื่น ดังนั้นการเข้าถึงระบบคอมพิวเตอร์จึงเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งการเข้าถึงระบบคอมพิวเตอร์ที่เป็นความผิดสำเร็จนั้นจะต้องเป็นการกระทำที่ก่อให้เกิดการทำงานของเครื่องคอมพิวเตอร์เป้าหมายหรือการเข้าถึงทางกายภาพตามที่ได้กล่าวมา การปฏิเสธการเข้าถึงโดยมาตรการป้องกันโดยเฉพาะก็น่าจะเป็นการเข้าถึงแล้ว

นอกจากนี้ ได้มีผู้ให้คำนิยามของคำว่า “การเข้าถึง (Access) ไว้ว่าเป็นการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้น จึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์หรือส่วนประกอบต่างๆของคอมพิวเตอร์ หรือข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจร เป็นต้น

อย่างไรก็ตาม “การเข้าถึง” ยังหมายความรวมถึงการเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆเครือข่ายเข้าด้วยกันและยังหมายถึงการเข้าถึงโดยผ่านระบบเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆกันเข้าด้วยกัน

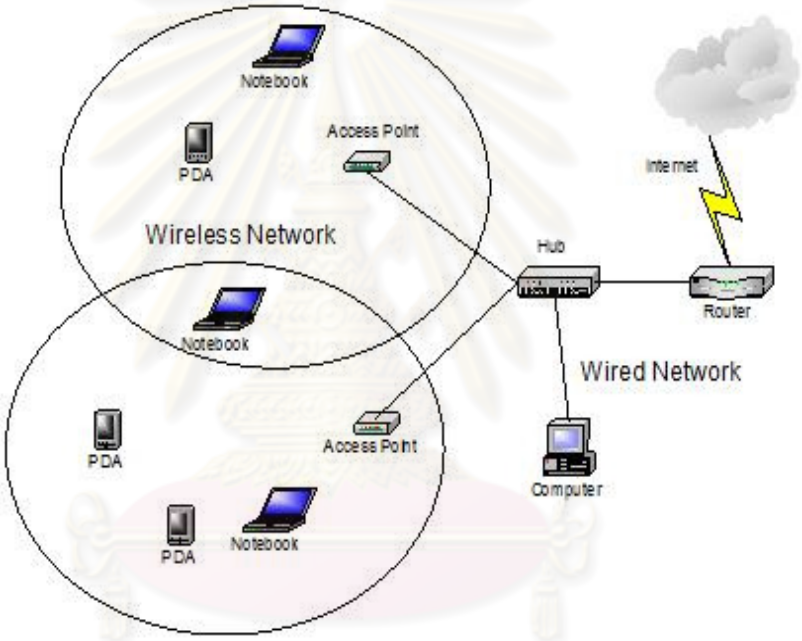
การที่กำหนดให้การเข้าถึงโดยปราศจากอำนาจหรือโดยฝ่าฝืนกฎหมาย และการใช้คอมพิวเตอร์ในทางมิชอบกระทำความผิดด้วยการเข้าถึงโดยไม่มีอำนาจหรือโดยฝ่าฝืนกฎหมาย ถือเป็นการกระทำที่คุกคามหรือเป็นภัยต่อความปลอดภัย (Security) ของระบบคอมพิวเตอร์และระบบข้อมูลที่มีผลกระทบต่อความครบถ้วน (Integrity) การรักษาความลับ (Confidential) และเสถียรภาพในการใช้งาน (Availability) ของระบบข้อมูลและระบบคอมพิวเตอร์ ซึ่งจะนำมาซึ่งความเสียหายหรือการกระทำผิดอื่นต่อไป ดังนั้นในหลายประเทศจึงได้มีการกำหนดให้การเข้าถึงโดยมิชอบเป็นความผิดขึ้น การเข้าถึงโดยไม่ได้รับอนุญาตนี้เกิดขึ้นเมื่อผู้กระทำประสบความสำเร็จในการเข้าสู่เป้าหมาย ซึ่งเป็นโปรแกรมหรือไฟล์คอมพิวเตอร์ ผู้กระทำอาจเป็นบุคคลหรือเป็นคอมพิวเตอร์ที่ถูกสั่งการให้กระทำโดยโปรแกรม การเข้าถึงอาจจะสำเร็จได้ด้วยวิธีทางอิเล็กทรอนิกส์ เช่น ผ่านทางรหัส (password) และโดยกลไกอื่นๆ หรือสำเร็จได้ด้วยทางกายภาพ เช่น การลักรหัสประจำตัว (personal identification) passwords (PIN)

การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบนี้ สามารถก่อให้เกิดความเสียหายแก่บุคคลเป็นส่วนตัวหรือแก่องค์กรโดยรวม เช่น การเข้าถึงข้อมูลส่วนบุคคลย่อมเป็นอันตรายต่อสิทธิส่วนบุคคล (privacy) ของผู้เสียหายหากว่าผู้กระทำนำเข้ามูลส่วนบุคคลนั้นไปเผยแพร่หรือจำหน่ายต่อให้แก่บุคคลที่สาม ในขณะที่การเข้าถึงระบบคอมพิวเตอร์ที่ใช้สำหรับการค้า ข้อมูลหรือความลับทางการค้าของบริษัทของผู้เสียหาย ย่อมเป็นอันตรายต่อการล่วงรู้โดยมิชอบต่อความลับทางการค้าของธุรกิจคู่แข่ง หากผู้กระทำนำข้อมูลดังกล่าวไปเผยแพร่หรือจำหน่ายต่อคู่แข่งทางการค้าของผู้เสียหาย

การลักลอบเข้าถึงระบบคอมพิวเตอร์นั้นสามารถกระทำได้ไม่ว่าผู้กระทำจะเป็นบุคคลภายในหรือภายนอกหน่วยงานก็ตาม โดยปกติแล้วเกือบทุกหน่วยงานจะมีการจำกัดอำนาจและเวลาของการเข้าถึงระบบสำหรับบุคคลในหน่วยงานไว้ หากผู้กระทำได้กระทำนอกเหนืออำนาจหรือเวลาโดยอาศัยโอกาสที่เหมาะสมเพื่อกระทำการโดยปราศจากการอนุญาตให้เข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) จะเรียกการกระทำในลักษณะนี้ว่า “การกระทำเกินกว่าอำนาจแห่งการเข้าถึง” (Exceeds Authorized Access)

เมื่อพิจารณาการกระทำอันเป็นการลักลอบเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) แล้วจะพบว่าเป็นการกระทำที่มีลักษณะเป็นการ “เข้าถึง” ตามคำนิยามที่ได้อ้างถึงข้างต้น เนื่องจากผู้ลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายหรือผู้บุกรุกจะนำอุปกรณ์ไร้สายของตนเข้าทำการเชื่อมต่อในขอบเขตที่ Access Point ส่งคลื่นวิทยุถึงและสามารถเข้าใช้บริการ

อินเทอร์เน็ตผ่านระบบเครือข่ายไร้สาย (Wireless LAN) ที่ตนเชื่อมต่อได้ โดยการกระทำดังกล่าวที่เรียกว่าเป็นการ “เข้าถึง” ระบบคอมพิวเตอร์เพราะเมื่ออุปกรณ์ไร้สายมีการเชื่อมต่อกับ Access Point ข้อมูลต่างๆ เช่น การร้องขอเปิดเว็บไซต์ การร้องขอใช้บริการอีเมล์ จากอุปกรณ์ไร้สายจะถูกส่งผ่าน Access Point ไปยังระบบอินเทอร์เน็ตต่อไป ซึ่ง Access Point ถือเป็นอุปกรณ์ชิ้นหนึ่งในระบบคอมพิวเตอร์เนื่องจากเป็นอุปกรณ์ที่เชื่อมการทำงานระหว่างอุปกรณ์ไร้สายเข้าด้วยกันกับระบบเครือข่ายใช้สาย (Wired LAN) ในการส่งผ่านข้อมูลจากอุปกรณ์ไร้สายผ่านเครือข่ายใช้สายไปสู่ระบบอินเตอร์เน็ต โดยที่การทำงานของ Access Point เป็นไปโดยอัตโนมัติ ดังรูปดังต่อไปนี้



ทั้งนี้ การเข้าถึงระบบคอมพิวเตอร์ของอุปกรณ์ไร้สายผ่าน Access Point ไปยังเครือข่ายอินเทอร์เน็ต ไม่ต้องคำนึงว่าระบบคอมพิวเตอร์นั้นจะมีการจัดการระบบรักษาความปลอดภัยในการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) หรือไม่ เพราะหากเชื่อมต่อกับ Access Point ก็ถือว่าเป็นการเข้าถึงระบบคอมพิวเตอร์แล้ว

3.1.2 การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย

ระบบเครือข่ายไร้สาย (Wireless LAN) ใช้สัญญาณคลื่นวิทยุในการสื่อสารข้อมูลระหว่าง Access Point กับอุปกรณ์ไร้สายแต่ละตัวที่มาเชื่อมต่อเข้ากับ Access Point เป็นเครือข่ายไร้สาย (Wireless LAN) หน่วยหนึ่งที่เรียกว่า Service Set ตามที่ได้กล่าวไว้แล้ว ในส่วนนี้

จะได้อธิบายให้ทราบต่อไปว่า สัญญาณคลื่นวิทยุที่ใช้ในระบบเครือข่ายไร้สาย (Wireless LAN) มีช่องความถี่เป็นอย่างไรเพราะเป็นประเด็นสำคัญที่เกี่ยวกับประสิทธิภาพในการรับ – ส่งข้อมูลในเครือข่ายไร้สาย (Wireless LAN)

ในช่วงความถี่ของคลื่นวิทยุ ซึ่งอยู่ในช่วงความถี่ 2.4 กิกะเฮิร์ต (GHz) นั้นเป็นความถี่ย่านสากลที่เครื่องใช้ไฟฟ้าหลายชนิดสามารถใช้ความถี่นี้ในการรับ – ส่งข้อมูลได้ ซึ่งอาจจะทำให้อุปกรณ์ไฟฟ้าเหล่านี้มีโอกาสที่จะรบกวนกันเองได้สูง ดังนั้น การแก้ไขปัญหานี้ทำได้โดยวิธีการมอดูเลชั่น[16] (Modulation) แบบ Spread Spectrum ที่จะมีการกระจายข้อมูลออกไปในช่วงต่างๆของย่านความถี่นี้ หากมีสัญญาณใดมารบกวนที่ความถี่หนึ่งๆก็จะเป็นเพียงจุดเล็กๆเท่านั้น ไม่ได้ทำให้การสื่อสารถูกตัดขาดลงไป เนื่องจากยังมีข้อมูลอื่นๆที่เหลืออยู่ในช่วงที่ส่งสัญญาณนี้ เมื่อผู้รับได้รับข้อมูลก็จะใช้ข้อมูลที่เหลือกู้ข้อมูลที่สูญหายไปได้

เทคนิคการมอดูเลชั่น (Modulation) แบบ Spread Spectrum นี้ทำให้คลื่นสัญญาณมีความทนทานต่อสัญญาณรบกวนในรูปแบบต่างๆได้ดีไม่ว่าจะเป็นปัญหาจากคลื่นสะท้อน (Multipath Interference) โดยมีเทคนิคการมอดูเลชั่น (Modulation) ที่นิยมใช้เป็นเทคนิคแบบ DSSS (Direct Sequence Spread Spectrum) ซึ่งจะใช้ความกว้างของเส้นทางในการรับ - ส่งข้อมูล (Bandwidth) 22 เมกะเฮิร์ต (MHz) แต่ในย่านความถี่ 2.4 กิกะเฮิร์ต (GHz) ซึ่งเป็นย่านของคลื่นวิทยุนั้นมี Bandwidth เพียง 83 เมกะเฮิร์ต (MHz) เท่านั้น ทำให้สามารถแบ่งช่องสัญญาณที่ใช้ในการสื่อสารเป็นช่องที่ไม่ซ้อนทับกันได้เพียง 3 ช่อง ส่วน Bandwidth ที่เหลือจะเว้นไว้เพื่อป้องกันการรบกวนกันระหว่างช่องสัญญาณต่างๆ[17]

---

[16] การโมดูเลชั่น(Modulation) คือการผสมสัญญาณข้อมูลเข้ากับสัญญาณความถี่สูง เช่นคลื่นวิทยุ ทำให้เดินทางได้ไกลขึ้นและป้องกันไม่ให้สัญญาณข้อมูลถูกรบกวน การโมดูเลชั่นสัญญาณแบ่งเป็น 2 กลุ่มใหญ่คือแบบอนาล็อค (Analog) และแบบดิจิทัล (Digital) (อ้างใน ACNETECH, “Modulation,” [ออนไลน์], 10 ธันวาคม 2553. แหล่งที่มา : http://www.acentech.net/cms/index.php?option=com_content&task=view&id=4 2 8 &Itemid=205)

[17] อรรณพ ขันธิกุลและอำนาจ มีมงคล, <u>ออกแบบและติดตั้งเครือข่าย Wireless LAN</u> (นนทบุรี : ไอดีซีฯ, 2547)

ดังนั้น เมื่อช่องความถี่แต่ละช่องมี Bandwidth 22 เมกะเฮิร์ต (MHz) หากมีการเข้าใช้บริการอินเทอร์เน็ตโดยผู้ใช้จำนวนหลายรายย่อมส่งผลให้ Bandwidth มีจำนวนไม่เพียงพอกับการใช้งานจนเกิดความล่าช้าของการใช้งานสามารถเปรียบเทียบได้กับเลนถนน ยิ่งมีเลนกว้างเท่าไรรถยนต์ซึ่งเปรียบได้กับข้อมูลก็สามารถวิ่งได้สะดวกมากขึ้นเท่านั้น แต่หากรถยนต์วิ่งบนถนนมากย่อมทำให้การจราจรคับคั่ง ซึ่งอย่างที่ได้ทราบแล้วว่า การรับ – ส่งข้อมูลระหว่างอุปกรณ์ไร้สายและ Access Point นั้น ตัวอุปกรณ์ไร้สายจะทำการฟังว่าสื่อในขณะนั้นว่างพร้อมที่ตัวอุปกรณ์ไร้สายจะส่งข้อมูลได้หรือไม่ หากยังไม่ว่างอุปกรณ์ไร้สายชิ้นนั้นก็จะทำการสุ่มเวลาเพื่อรอส่งข้อมูลต่อไป ดังนั้น หากมีอุปกรณ์ไร้สายเข้าใช้งานพร้อมๆกัน ย่อมทำให้สื่อไม่ว่างที่จะรับ – ส่งข้อมูลได้โดยทันทีแต่อุปกรณ์ไร้สายจะต้องสุ่มเวลาและรอเพื่อส่งข้อมูล ซึ่งจะทำให้การใช้งานในเครือข่ายไร้สาย (Wireless LAN) เป็นไปอย่างไม่คล่องตัวนัก

เห็นได้ว่าหากเกิดกรณีมีผู้ลักลอบเข้ามาใช้บริการอินเทอร์เน็ตในเครือข่ายไร้สาย (Wireless LAN) เพื่อเชื่อมต่อผ่านไปยังระบบอินเทอร์เน็ตแล้ว ย่อมส่งผลโดยตรงให้ระบบเครือข่ายไร้สาย (Wireless LAN) รับ – ส่งข้อมูลได้ช้าลง ซึ่งผลกระทบดังกล่าวย่อมส่งผลให้ผู้มีสิทธิใช้งานที่ชำระค่าบริการอินเทอร์เน็ตถูกต้องไม่ได้รับประโยชน์จากการใช้งานได้อย่างเต็มที่ เนื่องจากอาจเกิดความล่าช้าของระบบเพราะการติดขัดของการรับ – ส่งข้อมูล อีกทั้ง หากผู้ให้บริการอินเทอร์เน็ต (ISP) คิดค่าใช้บริการอินเทอร์เน็ตโดยอาศัยการคิดคำนวณตามปริมาณจากใช้งานที่แท้จริงแล้ว[18] แน่นอนว่าผู้มีสิทธิใช้งานที่ถูกลักลอบใช้งานจะต้องเสียค่าใช้จ่ายเป็นจำนวนที่มากขึ้นเกินกว่าที่ตนได้ใช้บริการอินเทอร์เน็ตไปตามความเป็นจริง

---

[18] ในปัจจุบันนี้ ปกติแล้วการคิดค่าบริการอินเทอร์เน็ต จะเป็นแบบเหมาจ่ายรายเดือนตามระดับความเร็วที่ผู้ใช้บริการจดทะเบียนไว้ซึ่งผู้ใช้บริการจะใช้งานมากน้อยเพียงใดก็ได้ การคิดค่าบริการตามจำนวนการใช้งานที่แท้จริง ส่วนใหญ่จะอยู่บนเครือข่ายผู้ให้บริการโทรศัพท์มือถือ (GPRS/EDGE และผู้ให้บริการบางรายจะผนวก WI-FI เข้าไปด้วย) (สัมภาษณ์ ฤทธิไกร ขัณฑวีระมงคล, ผู้ก่อตั้งเว็บไซต์ http://www.adslthailand.com, วันที่ 25 ธันวาคม 2553)

3.1.3 การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์เพื่อกระทำความผิด

ตามที่ได้กล่าวไว้แล้วว่า การใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายสามารถทำได้โดยง่ายเพียงแต่นำอุปกรณ์ไร้สาย เช่น โน้ทบุ๊ค (Notebook) เข้าไปอยู่ภายในขอบเขตที่อุปกรณ์กระจายสัญญาณไร้สาย (Access Point) กระจายคลื่นวิทยุออกมา เมื่ออุปกรณ์ไร้สายได้รับข้อมูลการเข้าใช้งานจาก Access Point แล้ว อุปกรณ์ไร้สายก็จะทำการเชื่อมต่อเข้าถึงระบบอินเทอร์เน็ตต่อไป

การเชื่อมต่อเพื่อเข้าใช้งานระบบอินเทอร์เน็ต มีอุปกรณ์บางชนิดเช่น Router ทำหน้าที่ในการแจก IP Address ให้เครื่องลูกข่ายทำให้เครื่องลูกข่ายสามารถใช้งานได้พร้อมกัน ซึ่ง IP Address ที่ Router แจกให้กับเครื่องลูกข่ายเป็น IP Address ภายในเครือข่าย (Private IP Address) ไม่ใช่ IP Address ได้รับจากผู้ให้บริการ เพราะ IP Address ที่ได้รับจากผู้ให้บริการจะเป็น IP Address ที่แท้จริงที่เรียกว่า Public IP Address นั่นเอง

ในบางครั้ง ผู้ลักลอบใช้บริการอินเทอร์เน็ตโดยอาศัยเครือข่ายไร้สายของผู้มีสิทธิใช้งาน อาจอาศัยเครือข่ายไร้สายนั้นเพื่อใช้บริการอินเทอร์เน็ตไปในทางเป็นความผิดต่อกฎหมาย เช่น นำภาพลามกอนาจารไปเผยแพร่ในระบบอินเทอร์เน็ต ลักข้อมูลบัตรเครดิต หรือใช้บริการอินเทอร์เน็ตในการฉ้อโกงบุคคลอื่น หากมีการตรวจสอบถึงการกระทำความผิดดังกล่าว เจ้าพนักงานมีอำนาจเรียกดูข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการอินเทอร์เน็ต (ISP) ว่าในขณะเกิดการกระทำความผิดผู้ให้บริการอินเตอร์เน็ตได้จัดสรร IP Address ให้แก่ผู้ใช้บริการ (เจ้าของเครือข่ายไร้สาย) รายใด[19] และในระบบเครือข่ายไร้สาย ผู้ใช้บริการซึ่งเป็นผู้มีสิทธิใช้งานที่

---

[19] ตามมาตรา 18 (2) แห่งพระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งได้บัญญัติไว้ว่า “ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

แท้จริงอาจจัดสรร IP Address ที่ได้รับมาจากผู้ให้บริการอินเตอร์เน็ตแก่เครื่องคอมพิวเตอร์ลูกข่ายเครื่องใดเครื่องหนึ่งก็ได้ เพราะระบบการจัดสรร IP Address ให้แก่เครื่องคอมพิวเตอร์ลูกข่ายโดยอุปกรณ์ Router เป็นไปโดยอัตโนมัติ (กระบวนการ NAT ตามหัวข้อที่ 2.2.3) ดังนั้นในกรณีของเครือข่ายไร้สาย หากผู้ใช้บริการไม่ได้ตั้งมาตรการความปลอดภัยในการเข้าถึงเครือข่ายไร้สายไว้ อุปกรณ์ไร้สายที่อยู่ในขอบเขตของสัญญาณก็สามารถเชื่อมต่อเข้าถึงระบบอินเทอร์เน็ตโดยอาศัยเครือข่ายไร้สายได้ทันที ซึ่งในบางครั้งการตรวจสอบในระบบเครือข่ายภายในของผู้ใช้บริการเองไม่อาจจะตรวจสอบได้ว่าในช่วงเวลาดังกล่าวอุปกรณ์ไร้สายลูกข่ายเครื่องใดเป็นผู้กระทำความผิด เนื่องจากว่าผู้ใช้บริการเกือบทุกรายโดยเฉพาะอย่างยิ่งผู้ที่ใช้บริการอินเทอร์เน็ตทั่วๆไปไม่ได้เก็บข้อมูลจราจรคอมพิวเตอร์ไว้นั่นเอง ทั้งนี้ จากการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งมีจุดมุ่งหมายเพื่อบัญญัติการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ กำหนดแนวปฏิบัติในทิศทางเดียวกันสำหรับผู้ที่เกี่ยวข้องกับระบบสารสนเทศหรือระบบคอมพิวเตอร์ และกำหนดให้ต้องมีการเก็บข้อมูลที่บันทึกเหตุการณ์ที่เกิดขึ้นบนระบบคอมพิวเตอร์ ข้อมูลดังกล่าวนี้ได้นิยามว่าเป็น “ข้อมูลจราจรคอมพิวเตอร์” และ “ข้อมูลผู้ใช้บริการ” และเพื่อกำหนดความชัดเจนเพิ่มเติม ได้ประกาศลงในราชกิจจานุเบกษาเรื่องประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เมื่อวันที่ 23 สิงหาคม 2550 เพื่อขยายความหลักเกณฑ์ทางเทคนิคในการเก็บข้อมูลจราจรคอมพิวเตอร์ เพื่อให้ผู้ให้บริการในแต่ละประเภทได้เก็บข้อมูลดังกล่าวและสามารถนำมาใช้ต่อไปได้[20]

ซึ่งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูล

---

[20] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (Nectec), “แนวทางการจัดเก็บข้อมูลล็อกสำหรับองค์กรเพื่อให้สอดคล้องตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550,” [ออนไลน์], 25 เมษายน 2554. แหล่งที่มา : http://www.thaicert.nectec.or.th/paper/auditing/LogImplementationandAuditingGuideline_r2.pdf

จราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ได้กำหนดนิยามของ “ผู้ให้บริการ” และ” ผู้ใช้บริการ” รวมถึงวางหลักเกณฑ์ให้ผู้ให้บริการมีหน้าที่ต้องเก็บข้อมูลจราจรคอมพิวเตอร์

1. **ผู้ให้บริการ** หมายความว่า

(1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

2. **ผู้ใช้บริการ** หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

ทั้งนี้ ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ได้กำหนดประเภทของผู้ให้บริการที่มีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังต่อไปนี้

1. ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าถึงอินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ 4 ประเภท ดังนี้

ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) เช่น ผู้ให้บริการโทรศัพท์พื้นฐาน, ผู้ให้บริการโทรศัพท์เคลื่อนที่, ผู้ให้บริการวงจรเช่า, ผู้ให้บริการ ADSL, ผู้ให้บริการดาวเทียม เป็นต้น

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) เช่น ผู้ให้บริการอินเทอร์เน็ตทั้งแบบมีสายและไร้สาย, ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรมหรือร้านอาหารและเครื่องดื่ม, ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือสถาบันการศึกษา เป็นต้น

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ(Host Service Provider) เช่น ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting), ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ เป็นต้น

ง. ผู้ให้บริการร้านอินเทอร์เน็ต

2. ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม1. ได้แก่ ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่าง ๆ (Content and Application Service Provider) เช่น ผู้ให้บริการเว็บบอร์ด (Webboard) หรือผู้ให้บริการบล็อค (Blog) เป็นต้น

ดังนั้น เป็นที่สังเกตได้ว่า ผู้ใช้บริการอินเทอร์เน็ตตามบ้านเรือนที่สมัครเป็นสมาชิกของผู้ให้บริการ แม้จะดำเนินการให้ระบบคอมพิวเตอร์ของตนสามารถเชื่อมต่ออินเทอร์เน็ตได้มากกว่า 1 เครื่อง ก็ไม่มีลักษณะเป็น “ผู้ให้บริการ” แต่อย่างใด โดยมีลักษณะเป็นแต่เพียง “ผู้ใช้บริการ” เท่านั้นจึงไม่มีหน้าที่ที่จะต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ตามบทบัญญัติของกฎหมาย

3.2 วิเคราะห์กฎหมายไทยที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตโดยมิชอบ

การพิจารณาการกระทำความผิดที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตโดยมิชอบกับความผิดตามประมวลกฎหมายอาญาแล้ว ก็คงจะปรับได้กับความผิดฐานลักทรัพย์และฐานบุกรุก ซึ่งในความผิดทั้งสองฐานนี้ ก็ไม่น่าจะมีปัญหาในการบังคับใช้กฎหมายหากเป็นกรณีที่การกระทำนั้นได้กระทำต่อตัวเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่างๆที่เป็นส่วนประกอบของคอมพิวเตอร์อันสามารถมองเห็นได้ด้วยทางกายภาพ หรือผู้กระทำต้องเข้าไปในอาคารศูนย์คอมพิวเตอร์แห่งนั้น แต่ในความเป็นจริงการใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายนั้น สิ่งที่ถูกลักลอบใช้งานไปหรือสิ่งที่อำนวยให้เกิดการใช้บริการอินเทอร์เน็ตเป็นสิ่งที่ไม่สามารถมองเห็นได้โดยทางกายภาพ การปรับใช้ประมวลกฎหมายอาญาในกรณีที่เกิดขึ้นจึงก่อให้เกิดปัญหาในการตีความ และในปัจจุบันนี้แม้ว่าจะมีกฎหมายเฉพาะ คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ใช้บังคับกับการลักลอบเข้าถึงระบบคอมพิวเตอร์โดยไม่ชอบด้วยกฎหมายแล้ว แต่การลักลอบเข้าถึงระบบคอมพิวเตอร์ตามที่พระราชบัญญัติฉบับดังกล่าวประสงค์จะคุ้มครอง ก็คุ้มครองเฉพาะแต่เพียงการการลักลอบเข้าถึงระบบคอมพิวเตอร์ซึ่งมีมาตรการป้องกันการเข้าถึงโดยเฉพาะเท่านั้น ซึ่งการลักลอบเข้าถึงระบบคอมพิวเตอร์ที่ไม่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ เจ้าของเครือข่ายไร้สายจะไม่ได้รับการคุ้มครองตามกฎหมายแต่อย่างใด จึงอาจทำให้เกิดปัญหาได้ว่า หากมีกรณีพิพาทเกิดขึ้นกับการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ที่ไม่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะแล้วจะมีการบังคับใช้กฎหมายอย่างไรหรือหากเป็นกรณีที่เจ้าของเครือข่ายไร้สาย (Wireless LAN) ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงระบบเครือข่ายไร้สายของตนและปรากฏว่ามีผู้ลักลอบใช้เครือข่ายไร้สายในการกระทำ

ความผิด เช่น ใช้อินเทอร์เน็ตของเจ้าของเครือข่ายไร้สายในการดาวน์โหลด (Download) โปรแกรมละเมิดลิขสิทธิ์ หรืออัพโหลด (Upload) ภาพลามกอนาจารเข้าถึงระบบอินเทอร์เน็ต เป็นต้น จะใช้บทบัญญัติกฎหมายใดบังคับกับกรณีที่เกิดขึ้นและเจ้าของเครือข่ายไร้สายจะต้องมีความรับผิดหรือไม่ เพียงใด

3.2.1 กรณีการลักลอบเข้าถึงระบบโดยมิชอบ

ความผิดในการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบนั้นเป็นการกระทำความผิดเกี่ยวกับการรักษาความลับ ความครบถ้วนและการทำงานของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ จึงถือเป็นการกระทำที่คุกคามหรือเป็นอันตรายต่อความปลอดภัย (Security) ของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ เมื่อระบบไม่มีความปลอดภัยก็จะส่งผลต่อความครบถ้วน การรักษาความลับ และความพร้อมหรือเสถียรภาพในการใช้งานของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์[21]ซึ่งเป็นฐานความผิดพื้นฐานในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั่นเอง ในส่วนความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้น นานาประเทศและนักกฎหมายโดยทั่วไปต่างเห็นพ้องต้องกันว่าการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อบุคคลโดยส่วนรวมและต่อสังคมและอาจส่งผลกระทบในวงกว้างทั้งในแง่สังคม เศรษฐกิจหรือแม้กระทั่งการเมือง

ประเด็นที่มีความแตกต่างและเป็นที่ถกเถียงกันคือ การเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ในระดับใดที่ควรเป็นความผิดทางอาญาและต้องถูกลงโทษ หากเพียงแค่มีการเข้าถึงโดยไม่ได้รับอนุญาตจะถือว่าเป็นการก่ออาชญากรรมได้หรือไม่ หรือผู้กระทำจะต้องมีมูลเหตุจูงใจที่จะกระทำให้เกิดความเสียหายด้วย เช่น บุคคลซึ่งมิได้มีมูลเหตุจูงใจดังกล่าวแต่ต้องการทดลองวิชาจึงเข้าไปในระบบข้อมูลของบุคคลอื่นโดยมิได้มีมูลเหตุจูงใจที่จะก่อให้เกิดความเสียหาย กรณีดังกล่าวควรกำหนดให้ต้องรับผิดและมีบทลงโทษหรือไม่ และกรณีที่มีการเข้าถึงแม้โดยไม่มีมูลเหตุจูงใจที่จะก่อให้เกิดความเสียหายควรจะมีความรับผิดใดๆหรือไม่

---

[21] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, “แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์,” [ออนไลน์], 14 กันยายน 2552. แหล่งที่มา : http://www.etcommission.go.th/books/Cyber_crime.pdf

การกำหนดฐานความผิดดังกล่าวมีความแตกต่างกันไปในแต่ละประเทศ โดยในประเทศที่กำหนดให้เป็นความผิดทันทีเมื่อมีการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ได้แก่ อังกฤษ มาเลเซีย สิงคโปร์ อิสราเอล ฝรั่งเศส ส่วนในบางประเทศได้กำหนดให้ผู้กระทำต้องรับโทษหนักขึ้นหากการเข้าถึงดังกล่าวได้ก่อให้เกิดความเสียหายหรือเป็นการกระทำผิดโดยมีเจตนาเพื่อกระทำความผิดอื่นต่อไป อาทิ ออสเตรเลีย ฝรั่งเศส อิตาลี นอรเวย์ สิงคโปร์

ส่วนประเทศที่กำหนดให้การเข้าถึงโดยมิชอบเป็นความผิดต่อเมื่อได้ละเมิดระบบการรักษาความมั่นคงเพื่อความปลอดภัยของระบบคอมพิวเตอร์ได้แก่ ประเทศเยอรมัน อิตาลี ออสเตรเลีย เนเธอร์แลนด์ สวิตเซอร์แลนด์ ในขณะเดียวกันก็มีบางประเทศที่กำหนดให้ผู้กระทำต้องรับผิดหนักขึ้นหากการเข้าถึงดังกล่าวเป็นการละเมิดระบบรักษาความมั่นคง เช่น โปรตุเกส

ดังนั้นพอจะสรุปได้ว่า แนวทางการบัญญัติความผิดฐานเข้าถึงโดยมิชอบมีอยู่ด้วยกัน 3 แนวทาง[22] กล่าวคือ

แนวทางที่ 1 กำหนดให้เป็นความผิดทันทีเมื่อมีการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบ

แนวทางที่ 2 กำหนดให้เป็นความผิดเฉพาะแต่กรณีที่ได้ละเมิดหรือฝ่าฝืนระบบการรักษาความมั่นคงหรือปลอดภัยเท่านั้น

แนวทางที่ 3 กำหนดให้ผู้กระทำต้องรับผิดหนักขึ้นหากการเข้าถึงดังกล่าวเป็นการละเมิดระบบรักษาความมั่นคงหรือปลอดภัย

สำหรับในประเทศไทย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดให้การเข้าถึงเป็นความผิด แม้ว่าผู้กระทำจะมิได้มีมูลเหตุจูงใจเพื่อก่อให้เกิดความเสียหายหรือการกระทำดังกล่าวจะยังมิได้ก่อให้เกิดความเสียหายก็ตาม เพียงแต่การเข้าถึงนั้นจะต้องเป็นการเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงไว้

---

[22] เรื่องเดียวกัน,

โดยเฉพาะ ทั้งนี้ เพราะเห็นว่าการกระทำดังกล่าวนั้นสามารถก่อให้เกิดการกระทำผิดฐานอื่นหรือฐานที่ใกล้เคียงค่อนข้างง่ายและอาจก่อให้เกิดความเสียหายร้ายแรง ทั้งการพิสูจน์มูลเหตุจูงใจทำได้ค่อนข้างยาก

มีความเห็น[23]ว่า ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้การเข้าถึงที่จะเป็นความผิดทางอาญานั้น ต้องเป็นความผิดในกรณีที่ได้ละเมิดหรือฝ่าฝืนระบบความมั่นคงหรือปลอดภัยที่มีการป้องกันโดยเฉพาะเท่านั้น โดยเห็นว่าการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่เจ้าของไม่ได้มีการป้องกันไว้โดยเฉพาะแสดงว่าเจ้าของไม่ได้หวงห้ามหรือไม่มีเจตนาที่จะป้องกันไว้โดยเฉพาะ จึงไม่น่าจะเป็นความผิดอาญา

แต่อย่างไรก็ดีในทางกลับกัน การตั้งมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์เป็นวิธีการทางเทคนิคด้วย เนื่องจากเจ้าของเครือข่ายไร้สายจะต้องดำเนินการตั้งมาตรการป้องกันความปลอดภัยในอุปกรณ์กระจายสัญญาณไร้สาย ซึ่งปัจจุบันจะมักจะใช้ Router เป็นอุปกรณ์กระจายสัญญาณนี้[24] ในกรณีที่เจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ ระบบเครือข่ายไร้สายจะเป็นระบบเปิด กล่าวคือเป็นระบบเครือข่ายไร้สายที่ไม่มีมาตรการป้องกัน

---

[23] พิญดา เลิศกิตติกุล, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550), หน้า 108

[24] โดยปกติแล้วแอกเซสพอยต์จะทำหน้าที่ในการกระจายสัญญาณไร้สาย แต่การใช้งานเครือข่ายไร้สายในปัจจุบันมักจะใช้ Wireless ADSL Router หรือที่เรียกกันว่า All-in-one ก็คือการนำ ADSL Modem + Router + Wireless Access Point มารวมกันในอุปกรณ์ชิ้นเดียว

ถ้าผู้ใช้งานอินเทอร์เน็ตต้องการใช้เครือข่ายไร้สายภายในบ้าน ก็มักจะเลือกซื้อ Wireless ADSL Router เพราะราคาจะถูกกว่าซื้อ ADSL Router และ Wireless Access Point อีกทั้งการติดตั้งก็ยังทำได้ง่ายกว่าอีกด้วย

การเข้าถึงแต่อย่างใด (Unsecured Wireless LAN) เพราะในการผลิต Router ผู้ผลิตจะตั้งค่าให้ Router ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงเอาไว้ตั้งแต่ต้น[25] ผู้ใช้บริการอินเตอร์เน็ตจะต้องดำเนินการตั้งค่าเองหรือผู้ให้บริการ (ISP) จะต้องดำเนินการตั้งค่าให้หรือผู้ให้บริการ (ISP) จะต้องให้คำแนะนำในการตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายในคู่มือการติดตั้งอุปกรณ์ ดังนั้นหากผู้ใช้บริการอินเตอร์เน็ตซึ่งเป็นเจ้าของระบบเครือข่ายไร้สายไม่ทราบวิธีการตั้งค่ามาตรการป้องกันการเข้าถึงระบบเครือข่ายไร้สายของตน อีกทั้งไม่ทราบถึงผลเสียหายที่เกิดขึ้นต่อระบบคอมพิวเตอร์หากมิได้มีการตั้งมาตรการป้องกันการเข้าถึงไว้ ก็ยังน่าจะถือได้ว่า เจ้าของระบบเครือข่ายไร้สายไม่ได้หวงห้ามหรือให้ความยินยอมแก่ผู้อื่นในการเข้าถึงระบบคอมพิวเตอร์ของตน ทั้งนี้เพราะว่าการรับบริการอินเทอร์เน็ต ผู้ใช้บริการควรจะต้องเป็นผู้ที่มีความรู้ในการใช้บริการอยู่แล้วทั้งวิธีการใช้บริการอินเทอร์เน็ต รูปแบบการใช้บริการอินเทอร์เน็ต รวมถึงภัยอันตรายที่อาจจะเกิดขึ้นจากความไม่ระมัดระวังในการป้องกันระบบคอมพิวเตอร์ของตนเองไม่ว่าจะเป็นการถูกลักลอบใช้บริการอินเทอร์เน็ตจากผู้อื่นหรือการที่ผู้ลักลอบเข้าถึงระบบคอมพิวเตอร์เพื่อกระทำความผิดก็ตาม และอีกประการหนึ่งหากผู้ใช้บริการไม่ต้องการถูกลักลอบใช้บริการอินเทอร์เน็ต ก็เพียงแต่ตั้งมาตรการป้องกันการเข้าถึงไว้ซึ่งทำได้ง่ายกว่าการจะไปดำเนินการจับกุมผู้ที่ลักลอบเข้าใช้บริการอินเทอร์เน็ต

ส่วนกรณีที่เจ้าของเครือข่ายไร้สายทราบถึงวิธีการตั้งค่ามาตรการป้องกันการเข้าถึงระบบเครือข่ายไร้สายหรือทราบถึงผลเสียหายที่จะเกิดขึ้นหากไม่ตั้งมาตรการป้องกันดังกล่าวและมิได้ดำเนินการตั้งมาตรการป้องกัน ก็เป็นที่แน่นอนว่า ผู้ใช้บริการอินเตอร์เน็ตซึ่งเป็นเจ้าของเครือข่ายไร้สายไม่ได้หวงห้ามในการให้ผู้อื่นเข้ามาใช้งานในระบบเครือข่ายไร้สายของตน ผู้เข้าถึงระบบเครือข่ายของผู้นั้นก็จะไม่มีความผิดแต่อย่างใดเพราะการไม่ตั้งมาตรการป้องกันการเข้าถึงดังกล่าวถือได้ว่าเจ้าของเครือข่ายได้ให้ความยินยอมในการเข้าถึงระบบคอมพิวเตอร์ของตน

---

[25] ศึกษาจากการติดตั้งRouterหลายยี่ห้อ เช่น D – Link DWL – 2000 AP, D – Link DSL – G604T, LevelOne Wireless ADSL Router (WBR – 3407A), Linksys WAG54G, SMC7094WBRA เป็นต้น (อ้างใน thelordofwireless.com, [ออนไลน์], 10 มกราคม 2554. แหล่งที่มา : http://www.thelordofwireless.com)

เหตุที่พิจารณาได้ว่าการที่เจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงระบบเครือข่ายไร้สายของตนทั้งกรณีที่เจ้าของระบบเครือข่ายไร้สายทราบและไม่ทราบวิธีการตั้งมาตรการป้องกันการเข้าถึงระบบเครือข่ายไร้สายจนเป็นเหตุให้มีผู้ลักลอบเข้าใช้บริการอินเทอร์เน็ตเป็นการที่เจ้าของระบบเครือข่ายไร้สายได้ให้ความยินยอมแก่ผู้ลักลอบในการเข้าใช้บริการอินเทอร์เน็ต ซึ่งการให้ความยินยอมที่จะทำให้การกระทำนั้นไม่เป็นความผิดอาญาตามสุภาษิตโรมันที่ว่า “ความยินยอมทำให้ไม่เสียหาย” ความยินยอมนั้นต้องมีลักษณะสามประการดังต่อไปนี้[26]

1. **ความยินยอมนั้นจะต้องไม่ขัดต่อสำนึกในศีลธรรมอันดีของประชาชน** การกระทำใดจะเป็นการขัดต่อศีลธรรมอันดีหรือไม่นั้น ต้องดูตามความรู้สึกของบุคคลทั่วไปในท้องถิ่นในเวลาที่เกิดการกระทำนั้น ซึ่งในเรื่องนี้คงจะต้องพิจารณาคุณธรรมทางกฎหมาย (Rechtgut) ว่าข้อใดกฎหมายยอมให้สละได้ โดยคุณธรรมทางกฎหมายสามารถแยกออกได้เป็น 2 ประเภท คือ

1.1 **คุณธรรมทางกฎหมายที่เป็นส่วนรวม** เป็นกฎหมายเกี่ยวกับการรักษาความปลอดภัยต่างๆ เช่น กฎหมายคุ้มครองแรงงาน เป็นต้น ผู้ที่เป็นเจ้าของคุณธรรมจะสละไม่ได้เพราะกฎหมายดังกล่าวเป็นกฎหมายที่มุ่งให้เกิดความสงบแก่ส่วนรวมและความยุติธรรมในสังคม

1.2 **คุณธรรมทางกฎหมายที่เป็นส่วนตัว** ผู้เป็นเจ้าของคุณธรรมนี้อาจยอมให้ผู้อื่นละเมิดได้ แต่ต้องดูว่ากฎหมายนั้นมุ่งคุ้มครองเอกชนโดยส่วนตัวอย่างแท้จริงหรือไม่ เช่น ความผิดฐานฉ้อโกงหรือยักยอกทรัพย์ แต่ถ้ากฎหมายมิได้คุ้มครองเพียงตัวบุคคล แต่ยังมองถึงสังคมส่วนรวมด้วยแล้ว เช่น การฉ้อโกงประชาชน รวามยินยอมของผู้เสียหายก็ไม่ลบล้างความผิด

ดังนั้นในส่วนของความยินยอมในการให้ผู้อื่นเข้าถึงระบบเครือข่ายไร้สายของตนในการใช้บริการอินเทอร์เน็ต เป็นความยินยอมที่ไม่ขัดต่อสำนึกในศีลธรรมอันดีของประชาชนเพราะคุณธรรมทางกฎหมายในส่วนนี้เป็นของเจ้าของระบบเครือข่ายไร้สายเป็นส่วนตัวไม่ได้กระทบแก่ความสงบของส่วนรวมหรือกระทบแก่ความยุติธรรมแต่อย่างใด

2. **ความยินยอมนั้นจะต้องเกิดขึ้นโดยความบริสุทธิ์ใจ** โดยเสรีและชัดแจ้ง ปราศจากการข่มขู่ ล่อลวงหรือสำคัญผิด ในข้อนี้ปัญหามีอยู่ว่า ผู้ยินยอมจะต้องมีความรู้ความเข้าใจแค่ไหนจึงจะเรียกว่ามีการยินยอมโดยบริสุทธิ์ใจ กล่าวคือ ผู้กระทำจะต้องมีความเข้าใจถึงเนื้อหาสาระในการยินยอมของตน ดังนั้น การที่เจ้าของระบบเครือข่ายไร้สายไม่ได้ตั้งมาตรการ

---

[26] ทวีเกียรติ มีนะกนิษฐ, คำอธิบายกฎหมายอาญาภาคทั่วไป. (กรุงเทพมหานคร : วิญญูชน, 2551), หน้า 161 - 163

ป้องกันการเข้าถึงไว้ย่อมเป็นความยินยอมอันเกิดขึ้นโดยความบริสุทธิ์ใจแล้ว ทั้งนี้เพราะว่าเจ้าของเครือข่ายไร้สายน่าจะย่อมทราบดีว่าการไม่ตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของตนอาจจะส่งผลให้เกิดการลักลอบเข้าถึงเครือข่ายไร้สายได้โดยง่ายและเมื่อมีการบุกรุกเข้าถึงเครือข่ายไร้สายก็อาจจะส่งผลให้มีการลักลอบใช้ประโยชน์ได้ต่อไป

3. **ความยินยอมนั้นจะต้องมีอยู่ตลอดเวลาที่กระทำความผิด** ซึ่งในกรณีที่เจ้าของเครือข่ายไร้สายไม่ตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของตนไว้ ย่อมถือได้ว่าเป็นการยินยอมให้ผู้อื่นสามารถเข้าใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายได้ตลอดเวลา

3.2.2 กรณีการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย

การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายจะต้องมีการกระทำที่ผ่านเข้าถึงระบบคอมพิวเตอร์ของเจ้าของเครือข่ายไร้สายเนื่องจากนิยามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ให้นิยามของคำว่า “ระบบคอมพิวเตอร์” ว่าหมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบคอมพิวเตอร์” จึงได้แก่ ฮาร์ดแวร์และซอฟแวร์ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูลดิจิทัล (Digital Data) อันประกอบด้วย เครื่องคอมพิวเตอร์และอุปกรณ์รอบข้าง (Peripheral) ต่างๆในการรับเข้าหรือป้อนข้อมูล (store and record) ดังนั้น ระบบคอมพิวเตอร์จึงอาจเป็นอุปกรณ์เพียงเครื่องเดียวหรือหลายเครื่องอันมีลักษณะเป็นชุดเชื่อมต่อกัน ทั้งนี้ โดยอาจเชื่อมต่อกันผ่านระบบเครือข่ายและมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมที่กำหนดไว้และไม่มีการแทรกแซงโดยตรงจากมนุษย์ โดยมีการทำงานประมวลผลข้อมูลโดยอัตโนมัติ[27] ดังนั้นเครื่องคอมพิวเตอร์ที่ได้เชื่อมต่อกับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) และได้เชื่อมต่อกับ Modem สำหรับเชื่อมต่อสู่บริการอินเทอร์เน็ตย่อมถือเป็น “ระบบคอมพิวเตอร์”

---

[27] สำนักงานเลขาธิการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์. (กรุงเทพมหานคร : สำนักงานฯ, 2547), หน้า15-16

ดังนั้น หากผู้ลักลอบได้ใช้บริการอินเทอร์เน็ตของบุคคลอื่นโดยผ่านเครือข่ายไร้สายของบุคคลนั้นจึงเป็นการกระทำที่เข้าถึงระบบคอมพิวเตอร์เช่นเดียวกันเพราะการเชื่อมต่อจากอุปกรณ์ไร้สายของผู้ลักลอบไปยัง Access Point ของบุคคลอื่นจะมีการส่งข้อมูลจากอุปกรณ์ไร้สายไปยังเครื่อง Access Point เพื่อส่งต่อผ่านไปยัง Modem ผ่านคู่สายโทรศัพท์ไปยังระบบอินเทอร์เน็ตต่อไป ซึ่งในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดฐานความผิดในการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนให้เป็นความผิด แต่มิได้กำหนดว่าการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นเพื่อประสงค์จะลักลอบใช้บริการอินเทอร์เน็ตเป็นความผิดหรือไม่ จึงสมควรต้องวิเคราะห์ว่าการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายจะเป็นความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนหรือไม่และจะมีผลทางกฎหมายเป็นเช่นใด

ในบทบัญญัติดังกล่าวข้างต้นนั้น อาจแยกองค์ประกอบได้ดังนี้

1. ผู้ใด
2. เข้าถึงโดยมิชอบ
3. ระบบคอมพิวเตอร์
4. ที่มีมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

โดยองค์ประกอบของบทบัญญัตินี้ อาจแยกพิจารณาได้ดังต่อไปนี้

1. ผู้ใด

คำว่า “ผู้ใด” หมายถึงบุคคลธรรมดาทั่วๆไปไม่ว่าจะเป็นเพศใดก็ตามก็สามารถกระทำความผิดฐานนี้ได้ ส่วนกรณีของนิติบุคคลจะเห็นได้ว่านิติบุคคลโดยทั่วไปไม่สามารถกระทำผิดทางอาญาในลักษณะนี้ได้ คำว่า “ผู้ใด” จึงไม่ได้หมายถึงนิติบุคคลด้วยแต่อย่างใด ดังนั้นองค์ประกอบในส่วนนี้จึงเป็นความหมายตามปกติที่ปรากฏในประมวลกฎหมายอาญา

2. เข้าถึงโดยมิชอบ

คำว่า “การเข้าถึง” ในที่นี้ หมายความรวมถึง การเข้าถึงทั้งในระดับกายภาพ เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์และผู้กระทำผิด

ดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าคอมพิวเตอร์นั้นเอง และหมายรวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้

"การเข้าถึง" ในที่นี้จะหมายถึง การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ทั้งหมดหรือบางส่วนก็ได้ ดังนั้น จึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่างๆของคอมพิวเตอร์ ข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

นอกจากนั้น "การเข้าถึง" ยังหมายถึงการเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆเครือข่ายเข้าด้วยกันและยังหมายถึงการเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network) อันเป็นเครือข่ายที่เชื่อมคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆเข้าด้วยกัน นอกจากนี้ ยังหมายความรวมถึงการเข้าถึงโดยการติดต่อสื่อสารแบบไร้สาย (Wireless Communication) อีกด้วย[28]

การเข้าถึงเครือข่ายไร้สายซึ่งเป็นส่วนหนึ่งของระบบคอมพิวเตอร์นั้น โดยมากเจ้าของอุปกรณ์ไร้สายจะต้องทำการเลือกเครือข่ายไร้สายที่ตนต้องการเข้าถึงเสียก่อน เว้นเสียแต่ว่าเจ้าของอุปกรณ์ไร้สายนั้นจะได้ตั้งค่าปรับแต่งค่าให้เชื่อมต่อเครือข่ายไร้สายโดยอัตโนมัติทันทีที่ตรวจพบ (Automatically connect to non-preferred networks) ซึ่งส่วนใหญ่จะพบในระบบปฏิบัติการ Windows XP ที่ไปเปิดการใช้ฟังก์ชั่นดังกล่าวไว้[29]

"การเข้าถึง" ซึ่งถือเป็นความผิดฐานนี้ จะต้องเป็นการเข้าถึงโดยมิชอบด้วย ดังนั้นจึงต้องทำความเข้าใจเสียก่อนว่าคำว่า "โดยมิชอบ" มีความหมายอย่างไร ซึ่งคำว่า "โดยมิชอบ" ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ปรากฏอยู่ในส่วน "การเข้าถึงโดยมิชอบ" ถ้อยคำดังกล่าวค่อนข้างเป็นถ้อยคำที่คลุมเครือว่า "โดยมิชอบ" นั้น

---

[28] เรื่องเดียวกัน, หน้า 21

[29] สัมภาษณ์ ฤทธิไกร ขัณฑวีระมงคล ผู้ก่อตั้งเว็บไซต์

http://www.adslthailand.com, 25 ธันวาคม 2553

หมายถึงโดยมิชอบต่อหลักเกณฑ์อะไร ซึ่งหากพิจารณาองค์ประกอบตามประมวลกฎหมายอาญา มาตรา 320 วรรค2 ที่เกี่ยวกับการใช้บัตรอิเล็กทรอนิกส์โดยมิชอบ คำว่า “โดยมิชอบ” ได้มีคำอธิบายว่าคือ การกระทำที่มิชอบด้วยกฎหมาย ซึ่งมีความเห็นว่า[30]เป็นการแปลความที่แคบเกินไป เพราะในบางครั้งการเข้าถึงอาจจะเป็นการเข้าถึงโดยผิดต่อสัญญาก็ได้ ในเรื่องนี้กฎหมายอังกฤษได้วางองค์ประกอบกำกับการเข้าถึงว่า “โดยไม่ได้รับอนุญาต” ซึ่งองค์ประกอบดังกล่าวจะกว้างกว่าคำว่า “โดยมิชอบด้วยกฎหมาย” โดยรวมถึงการเข้าถึงที่ผิดต่อสัญญา แต่อย่างไรก็ตาม คำว่า “โดยมิชอบ” ก็น่าจะมีความหมายที่กว้างกว่าคำว่า “โดยไม่ได้รับอนุญาต” เนื่องจากหากฝ่ายนิติบัญญัติต้องการให้มีความหมายเช่นเดียวกับคำว่า โดยไม่ได้รับอนุญาตก็คงบัญญัติไว้เช่นนั้นแล้ว

หากพิจารณาตามคำพิพากษาฎีกาในคดีอาญา ได้กำหนดหลักเกณฑ์ในการตีความ คำว่า “โดยมิชอบ” ไว้อย่างกว้างหลายความหมาย เช่น ทุจริตต่อหน้าที่, ไม่ขวนขวายดำเนินการตามหน้าที่และระเบียบข้อบังคับ, มีเจตนาทุจริต, ละเว้นไม่ตรวจสอบความถูกต้องแท้จริง, ฝ่าฝืนคำสั่ง, ละเลยไม่ปฏิบัติหน้าที่ เป็นต้น โดยคำพิพากษาเหล่านี้เป็นความหมายของคำว่า “โดยมิชอบ” ตามมาตรา 157 แห่งประมวลกฎหมายอาญา โดยจะเห็นได้ว่ามีการตีความคำว่า “โดยมิชอบ” เป็นลักษณะของการกระทำอย่างกว้าง

ในส่วนของความเห็นทางวิชาการนั้นคำว่า “โดยมิชอบ” มีความเห็นเป็นสามแนวทาง ดังนี้

ความเห็นแนวทางที่หนึ่งเห็นว่า คำว่า “โดยมิชอบ” หมายถึง โดยมิชอบด้วยกฎหมาย

ความเห็นแนวทางที่สอง เห็นว่า คำว่า “โดยมิชอบ” เป็นถ้อยคำที่ไม่มีบัญญัติไว้ในประมวลกฎหมายอาญาหมวดคำนิยาม มาตรา 1 สมควรที่จะมีการกำหนดความหมายของคำว่า “โดยมิชอบ” โดยมีการเสนอให้บัญญัติให้สอดคล้องกับกฎหมายเดิมโดยกำหนดความหมายของคำว่า “โดยมิชอบ” หรือให้ใช้คำว่า “โดยทุจริต”

---

[30] ชาตรี ส่งสัมพันธ์, “อาชญากรรมคอมพิวเตอร์ : ศึกษาวิเคราะห์การเข้าถึงโดยมิชอบ,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2552), หน้า 106 - 110

ความเห็นแนวทางที่สาม เห็นว่า คำว่า “โดยมิชอบ” หมายถึง ไม่เหมาะสมหรือไม่ถูกต้อง

เมื่อพิจารณา “การเข้าถึงโดยมิชอบ” ที่สมควรจะเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 นี้แล้วคำว่า “โดยมิชอบ” ไม่ควรจะมีความหมายเฉพาะว่าการเข้าถึงโดยมิชอบนั้นเป็นการเข้าถึงโดยมิชอบด้วยกฎหมายเท่านั้นเพราะจะเป็นการแปลความหมายที่ค่อนข้างแคบเกินไป เนื่องจากหากเป็นการเข้าถึงที่ไม่มีกฎหมายห้ามแต่เป็นการเข้าถึงที่ไม่เหมาะสมหรือไม่ถูกต้องแล้ว ก็จะไม่เป็นความผิดแต่อย่างใด

การแปลความหมายของคำว่า “โดยมิชอบ” ควรจะแปลว่าหมายถึง การเข้าถึงโดยไม่เหมาะสมหรือไม่ถูกต้องเพราะเป็นการกำหนดความหมายไว้กว้างๆโดยให้เป็นดุลพินิจของผู้พิพากษาซึ่งเป็นการเหมาะสมเพราะผู้พิพากษาสามารถตีความคำว่า “โดยมิชอบ” ให้เหมาะสมกับยุคสมัยได้

3. ระบบคอมพิวเตอร์

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ให้นิยามคำว่า “ระบบคอมพิวเตอร์” ไว้ว่าหมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

เมื่อพิจารณาคำนิยามดังกล่าวข้างต้นจึงต้องวิเคราะห์ว่าระบบเครือข่ายไร้สายถือเป็นระบบคอมพิวเตอร์หรือไม่ เนื่องจากการกระทำอันเป็นความผิดจะต้องมีลักษณะเป็นการเข้าถึง”ระบบคอมพิวเตอร์” ซึ่งในระบบเครือข่ายไร้สายจะใช้ Access Point เป็นตัวเชื่อมในการสื่อสารข้อมูลระหว่างอุปกรณ์ไร้สายกับคอมพิวเตอร์หรือใช้ Access Point เป็นตัวเชื่อมในการสื่อสารข้อมูลระหว่างอุปกรณ์ไร้สายผ่านไปถึงระบบอินเทอร์เน็ต ดังนั้น Access Point จึงทำหน้าที่เป็นอุปกรณ์ที่เชื่อมการทำงาน โดย Access Point จะทำหน้าที่เชื่อมการทำงานโดยอัตโนมัติ จึงพอที่จะสรุปได้ว่า ระบบเครือข่ายไร้สายถือเป็นระบบคอมพิวเตอร์เช่นเดียวกัน

4. มีมาตรการการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

แม้ว่าโดยปกติแล้วการบัญญัติให้การเข้าถึงโดยมิชอบเป็นความผิดนั้นหลายฝ่ายมีความกังวลว่าเป็นจะเป็นการใช้กฎหมายอาญาเฟ้อหรือมีขอบเขตที่กว้างเกินสมควร แต่การกำหนดองค์องค์ประกอบความผิดเกี่ยวกับการล่วงล้ำมาตรการป้องกัน (infriging security measures) นั้นในหลายประเทศ[31]พบว่าเป็นการก่อให้เกิดปัญหาในการลงโทษผู้กระทำความผิดตามมา โดยการใช้ถ้อยคำดังกล่าวแม้จะเป็นการส่งเสริมให้ประชาชนใช้ระบบรักษาความปลอดภัยของคอมพิวเตอร์ของตนมากขึ้น แต่ในขณะเดียวกันรัฐก็จะเพิกเฉยที่จะดำเนินคดีกับผู้กระทำความผิดหากผู้กระทำความผิดได้เข้าไปในคอมพิวเตอร์ที่ไม่ได้ตั้งมาตรการป้องกันรักษาความปลอดภัยไว้เพราะการกระทำนั้นย่อมไม่เป็นความผิด

การกำหนดองค์ประกอบความผิดดังกล่าวนั้นมีความเห็นว่า[32]การกำหนดให้การล่วงล้ำมาตรการป้องกันรักษาความปลอดภัยเป็นองค์ประกอบความผิดด้วยนั้นไม่เหมาะสม เนื่องจากจะทำให้มีปัญหาในการตีความว่าอะไรคือมาตรการป้องกันการเข้าถึงโดยเฉพาะและอีกประการหนึ่งเป็นการผลักภาระทางอ้อมให้ประชาชนต้องเป็นผู้ดูแลรักษาคอมพิวเตอร์ของตนเอง ซึ่งสำหรับประชาชนทั่วไปที่ไม่ได้เป็นผู้มีความรู้ทางด้านคอมพิวเตอร์และคิดว่าตนเองไม่ได้มีสิ่งที่เป็นสาระสำคัญหรือประโยชน์อยู่ในระบบคอมพิวเตอร์ ย่อมไม่ทำการป้องกันและไม่อาจทราบได้ว่ากฎหมายจะไม่คุ้มครองตนเองหากว่าไม่มีมาตรการป้องกันการเข้าถึง

แต่อย่างไรก็ตามสำหรับองค์ประกอบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 ในส่วนที่เกี่ยวข้องกับมาตราการป้องกันรักษาความปลอดภัยของระบบคอมพิวเตอร์ อาจแยกองค์ประกอบในส่วนนี้ได้เป็น 2 ส่วน คือ

---

[31] Judge Stein Schjqlberg and Amanda M. Hubbard, “Background paper harmonizing national and legal approaches on cyber, “ [Online] Available from http://www.itu.int/osg/spuold/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (11 กุมภาพันธ์ 2554)

[32] Ibid.,

1. มาตรการป้องกันการเข้าถึงโดยเฉพาะ และ
2. มาตรการนั้นมิได้มีไว้สำหรับตน

โดยระบบคอมพิวเตอร์ใดที่เป็นระบบที่มีวิธีป้องกันการเข้าถึงโดยเฉพาะนั้น ผู้ร่างกฎหมายเห็นว่าเป็นข้อเท็จจริงที่จะต้องนำสืบเป็นเรื่องๆไป ส่วนเหตุผลที่บัญญัติองค์ประกอบความผิดนี้ก็เพราะมีระบบคอมพิวเตอร์จำนวนมากที่เจ้าของไม่ได้หวงแหนการที่บุคคลใดจะเข้าถึง[33] เมื่อมิได้หวงแหนแล้วกฎหมายจึงสันนิษฐานว่าระบบคอมพิวเตอร์นั้นไม่เป็นความลับเจ้าของระบบไม่ขัดขวางหากจะมีผู้หนึ่งผู้ใดเข้าถึงระบบคอมพิวเตอร์ของตน

หากพิจารณาจากองค์ประกอบในส่วน “มาตรการป้องกันการเข้าถึงโดยเฉพาะ” ว่าลักษณะอย่างไรจึงจะถือว่าเป็นระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะ เนื่องจากมีความหมายกว้างมาก เช่น คอมพิวเตอร์ส่วนบุคคลเครื่องหนึ่งไม่มีระบบรักษาความปลอดภัยของข้อมูลอยู่ในเครื่องเลย และก็ไม่ได้กำหนดรหัสผ่านสำหรับการเปิดดูข้อมูลตั้งอยู่ในบ้าน ในกรณีเช่นนี้จะถือว่าข้อมูลคอมพิวเตอร์มีวิธีการป้องกันการเข้าถึงโดยเฉพาะหรือไม่ หากมีคนเข้าไปเปิดดูข้อมูลจะมีความผิดหรือไม่ ซึ่งในกรณีนี้ตามบทบัญญัติของกฎหมายแล้วน่าจะพิจารณาได้ว่ามาตรการป้องกันการเข้าถึงโดยเฉพาะนั้นต้องเป็นมาตรการป้องกันในแง่ของระบบคอมพิวเตอร์นั้นเอง หากเป็นเครื่องคอมพิวเตอร์ที่ไม่มีระบบป้องกันในระบบของตนหากแต่มีการป้องกันทางกายภาพ เช่น มีการเอาสิ่งกีดขวางไปตั้งไว้ไม่ให้เข้าถึงเครื่องคอมพิวเตอร์หรือเก็บไว้ในห้องที่ปิดไว้ ไม่ถือว่าเป็นมาตรการป้องกันการเข้าถึงโดยเฉพาะแต่อย่างใด เนื่องจากไม่ใช่วิธีการทางด้านคอมพิวเตอร์ จึงไม่ถือว่าเป็นการเข้าถึงโดยมิชอบ เช่นเดียวกับกรณีที่มีการเก็บแผ่นดิสเกตต์หรือแฮนดี้ไดร์ฟที่ไม่มีการตั้งรหัสผ่านสำหรับการเข้าถึงข้อมูลไว้ในลิ้นชักแล้วใส่กุญแจไว้ ในกรณีเช่นนี้ไม่น่าจะถือว่าเป็นวิธีการป้องกันการเข้าถึงโดยเฉพาะเช่นกัน

เมื่อพิจารณาระบบเครือข่ายไร้สายแล้วจะเห็นได้ว่า “มาตรการป้องกันการเข้าถึงโดยเฉพาะ”นั้นน่าจะหมายถึงการที่เจ้าของเครือข่ายไร้สายได้กำหนดให้ระบบเครือข่ายไร้สายของตนระงับการประกาศชื่อเครือข่าย (Hide SSID) เพราะเมื่อเจ้าของเครือข่ายไร้สายได้ดำเนินการระงับการประกาศชื่อเครือข่ายแล้ว โปรแกรมในอุปกรณ์ไร้สายก็จะไม่ทราบว่ามีเครือข่ายไร้สาย

---

[33] พรเพชร วิชิตชลชัย, “คำอธิบาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550,” (กรุงเทพมหานคร : สำนักงานศาลยุติธรรม), หน้า 11

เครือข่ายนี้อยู่ในบริเวณที่อุปกรณ์ไร้สายสามารถเชื่อมต่อเข้าใช้งานได้ เมื่อผู้ใช้บริการต้องการใช้เครือข่ายไร้สายก็จะต้องทราบชื่อเครือข่ายไร้สายและทำการตั้งชื่อเครือข่ายในอุปกรณ์ไร้สายก่อนเข้าใช้งาน[34] หากผู้ลักลอบซึ่งไม่ใช่ผู้มีสิทธิใช้งานยังคงต้องการเข้าใช้งานในเครือข่ายไร้สายที่ได้ระงับการประกาศชื่อเครือข่ายไว้ก็จะต้องใช้โปรแกรมเพื่อดักฟังข้อมูลที่ส่งผ่านทางสัญญาณไร้สายเพื่อให้ทราบถึงชื่อเครือข่ายไร้สายเพื่อจะได้เข้าใช้งานต่อไป

ส่วนองค์ประกอบในแง่ “มาตรการนั้นมิได้มีไว้สำหรับตน” หมายถึง การป้องกันนั้นหากผู้ที่เข้าถึงมีอำนาจที่จะเข้าไปได้ ผู้นั้นก็ไม่มีความผิด เช่นลูกจ้างสามารถเข้าถึงข้อมูลของบริษัทนายจ้างได้เนื่องจากมีอำนาจหน้าที่ปฏิบัติงานในส่วนนั้น หรือกรณีเข้าไปโดยมีอำนาจ เช่น ผู้ดูแลเว็บไซต์ (Webmaster) เข้าไปดูแลระบบภายใต้อำนาจที่ตนมีอยู่ก็ไม่ถือว่ามีการกระทำผิด

ดังนั้น ในกรณีที่มีผู้ลักลอบเข้าถึงระบบเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะ หากพิจารณาตามตัวบทกฎหมายก็จะไม่มีความผิดแต่อย่างใด เพราะแม้ว่าการเข้าถึงเครือข่ายไร้สายของผู้อื่นอาจจะพิจารณาได้ว่าเป็นไปโดยมิชอบเนื่องจากผู้ลักลอบทราบดีว่าเครือข่ายไร้สายที่ตนเข้าถึงนั้นตนไม่มีสิทธิใช้บริการ จึงเป็นกรณีที่เข้าถึงโดยไม่เหมาะสมและไม่ถูกต้อง แต่อย่างไรก็ตาม เมื่อระบบเครือข่ายไร้สายนั้นไม่ได้ตั้มาตรการป้องกันการเข้าถึงไว้ การกระทำอันเป็นการเข้าถึงเครือข่ายไร้สายจึงไม่มีความผิดแต่อย่างใด

3.2.3 กรณีการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์เพื่อกระทำความผิด

ตามที่ได้กล่าวไว้แล้วว่า หากมีบุคคลใดก็ตามนำอุปกรณ์ไร้สายเข้ามาในขอบเขตที่เครื่องกระจายสัญญาณไร้สาย (Access Point) กระจายสัญญาณออกมา บุคคลนั้นสามารถใช้บริการอินเทอร์เน็ตของเจ้าของเครือข่ายไร้สายได้หากเจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะ โดยในระบบคอมพิวเตอร์ของเครือข่ายไร้สายจะจัดสรร IP Address ภายใน (Private IP Address) ให้แก่ อุปกรณ์ไร้สายที่ผู้ลักลอบนำมาเชื่อมต่อ ซึ่งก็จะมีวิธีการแปลง IP Address จาก IP Address ภายใน (Private IP Address) เป็น IP Address ที่

---

[34] อนันต์ ผลเพิ่ม, แลนไร้สาย (Wireless LAN), หน้า 126

สามารถเชื่อมต่อได้กับระบบอินเทอร์เน็ต (Public IP Address) หรือที่เรียกว่า กระบวนการ Network Address Translation (NAT) ที่ได้อ้างถึงในหัวข้อ 2.2.3

ดังนั้น เมื่อผู้ลักลอบสามารถใช้บริการอินเทอร์เน็ตได้ ผู้ลักลอบอาจจะใช้ระบบเครือข่ายไร้สายซึ่งถือเป็นระบบคอมพิวเตอร์ของเจ้าของเครือข่ายไร้สายที่แท้จริงกระทำความผิดทางอาญาได้ อาทิเช่น

- ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ
- กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้
- ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข
- นำเข้าถึงระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือด้วยวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชังหรือได้รับความอับอาย

หากมีการกระทำความผิดดังกล่าวเกิดขึ้นและผู้เสียหายได้ดำเนินการแจ้งความร้องทุกข์ต่อเจ้าพนักงานตำรวจ เจ้าพนักงานตำรวจมีอำนาจตามมาตรา 18 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในการเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้องซึ่งคำว่า “ข้อมูลจราจรทางคอมพิวเตอร์” มีนิยามศัพท์ไว้ในมาตรา 3 ของพระราชบัญญัติเดียวกันว่า หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

ดังนั้นคำว่า “ข้อมูลจราจรทางคอมพิวเตอร์” จึงหมายถึงข้อมูลที่แสดงรายการให้เห็นถึงการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ซึ่งจะแสดงถึงแหล่งกำเนิด เช่น IP Address ของเครื่อง ชื่อที่อยู่ของผู้ใช้บริการที่มีการลงทะเบียน ข้อมูลของผู้ให้บริการ (service provider) ลักษณะของการให้บริการว่าผ่านระบบใดหรือเครือข่ายใด วันเวลาของการส่งข้อมูลและข้อมูลทุกประเภทที่เกิด

จากการสื่อสาร (communication) ผ่าน “ระบบคอมพิวเตอร์” [35] ข้อมูลจราจรคอมพิวเตอร์นี้จะจัดเก็บโดยผู้ให้บริการซึ่งตามพระราชบัญญัติฉบับเดียวกัน ได้ให้คำนิยาม “ผู้ให้บริการ” ไว้ตามความหมายที่ได้กล่าวไว้แล้วในหัวข้อที่ 3.1.3

ดังนั้น จากนิยามศัพท์และความหมายของคำว่า “ข้อมูลจราจรคอมพิวเตอร์” และ “ผู้ให้บริการ” ผู้ให้บริการที่มีหน้าที่เก็บข้อมูลจราจรคอมพิวเตอร์มีทั้งผู้ให้บริการอินเทอร์เน็ต (ISP) และผู้ใช้บริการอินเทอร์เน็ตที่เป็นเจ้าของเครือข่ายไร้สายที่นำระบบเครือข่ายไร้สายมาให้ผู้อื่นใช้บริการอินเทอร์เน็ตอีกทอดหนึ่ง เช่น ให้บริการในห้องพัก ห้องเช่า โรงแรมหรือร้านอาหารและเครื่องดื่ม, ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือสถาบันการศึกษา ,ให้บริการร้านอินเทอร์เน็ต หรือผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคล เช่น ผู้ให้บริการเว็บบอร์ด (Webboard) หรือผู้ให้บริการบล็อค (Blog) เป็นต้น ดังนั้นผู้ใช้บริการที่เป็นสมาชิกของผู้ให้บริการอินเทอร์เน็ต (ISP) ที่ใช้งานตามบ้านเรือนแม้ว่าจะสามารถให้บุคคลอื่นใช้อุปกรณ์ไร้สายเชื่อมต่อเข้าถึงระบบเครือข่ายไร้สายภายในขอบเขตที่ Access Point กระจายสัญญาณเพื่อใช้งานอินเทอร์เน็ตไร้สายได้ก็ไม่มีหน้าที่ต้องเก็บข้อมูลจราจรคอมพิวเตอร์แต่อย่างใด[36]

ดังนั้น ผู้ให้บริการทั้งหลายตามความหมายของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีหน้าที่ต้องเก็บรวบรวมบันทึกข้อมูลจราจรคอมพิวเตอร์ว่า ในวันเวลาดังกล่าว IP Address ภายใน (Private IP Address) หมายเลขใด เข้าใช้บริการอินเทอร์เน็ตในเว็บไซต์หรือบริการใดบ้าง เพื่อที่จะใช้เป็นหลักฐานเพราะหากมีการกระทำความผิดเกิดขึ้นก็สามารถจะพิสูจน์ได้ว่า เครื่องลูกข่ายเครื่องใดเป็นผู้กระทำความผิด ส่วน

---

[35] พรเพชร วิชิตชลชัย, “คำอธิบาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550,” (กรุงเทพมหานคร : สำนักงานศาลยุติธรรม),หน้า 5

[36] แต่อย่างไรก็ตาม หากเป็นผู้ให้บริการที่มีหน้าที่ตามกฎหมายในการเก็บข้อมูลจราจรคอมพิวเตอร์ จะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าถึงระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษา ข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษ เฉพาะรายและเฉพาะคราวก็ได้ หากฝ่าฝืนจะต้องระวางโทษปรับไม่เกินห้าแสนบาท

ทางด้านผู้ให้บริการ (ISP) ก็จะเก็บข้อมูลจราจรคอมพิวเตอร์ในลักษณะที่ว่า ในช่วงเวลาดังกล่าวตนได้จัดสรร IP Address (Public IP Address) ให้แก่ผู้ใช้บริการ (เจ้าของระบบคอมพิวเตอร์) รายใด

แต่อย่างไรก็ตาม เป็นที่น่าสังเกตว่า เจ้าของระบบเครือข่ายไร้สายบางรายแม้มีหน้าที่ตามกฎหมายที่จะต้องเก็บข้อมูลจราจรคอมพิวเตอร์แต่ก็ไม่ได้เก็บข้อมูลจราจรคอมพิวเตอร์เอาไว้แต่อย่างใด เนื่องจากในอุปกรณ์ทำหน้าที่เก็บข้อมูลจราจรคอมพิวเตอร์ไว้มีเนื้อที่ในการเก็บข้อมูลที่มีจำนวนจำกัดและยังต้องตั้งค่าระบบให้บันทึกการจัดเก็บเอาไว้ในฮาร์ดดิส (Hard Disk) ซึ่งเจ้าของระบบคอมพิวเตอร์บางรายอาจจะไม่ทราบถึงวิธีการดังกล่าว

ในส่วนของการเก็บข้อมูลจราจรคอมพิวเตอร์ที่สื่อสารทางอินเทอร์เน็ตนั้น แน่นอนว่าทั้งเจ้าของระบบคอมพิวเตอร์ที่ตั้งค่ามาตรการป้องกันการเข้าถึงไว้และที่ไม่ได้ตั้งค่ามาตรการป้องกันการเข้าถึงไว้หากเป็นผู้ให้บริการตามความหมายของกฎหมายแล้วย่อมมีหน้าที่ที่จะต้องเก็บข้อมูลจราจรคอมพิวเตอร์ทั้งสิ้น ซึ่งหากพิจารณาให้ลึกซึ้งลงไปในปัญหาของการกระทำความผิดโดยอาศัยเครือข่ายไร้สายของผู้อื่นที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะนั้น เจ้าของเครือข่ายไร้สายที่ไม่ตั้งมาตรการป้องกันการเข้าถึงไว้ก็น่าจะต้องมีความรับผิดในการไม่ตั้งมาตรการป้องกันการเข้าถึงไว้ด้วยเนื่องจากส่งผลให้มีผู้ลักลอบเข้าถึงระบบได้โดยง่าย ซึ่งในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 15 บัญญัติให้ผู้ให้บริการผู้ใดที่จงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14[37] แต่มีข้อสังเกตว่า บทบัญญัติมาตรา 15 ใช้ถ้อยคำว่า “จงใจ” ซึ่งหมายถึงผู้ให้บริการต้องรู้ว่ามี

---

[37] มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าถึงระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าถึงระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าถึงระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

การกระทำความผิดตามมาตรา 14 เช่นมีการเตือนหรือแจ้งให้ทราบแล้วว่าข้อมูลคอมพิวเตอร์นั้นเป็นความผิดต่อกฎหมายตามบทบัญญัติมาตรา 14 แต่ผู้ให้บริการยังปล่อยให้มีการเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นความผิดในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ก็จะถือได้ว่าเป็นการจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิด[38]แต่หากเป็นกรณีเจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ โดยไม่ทราบว่ามีการกระทำความผิดก็จะไม่มีความผิดตามบทบัญญัติมาตรานี้แต่อย่างใด

ในส่วนของการลักลอบเข้าถึงระบบอินเทอร์เน็ตของเจ้าของเครือข่ายไร้สายเพื่อกระทำความผิดอื่น โดยการกระทำผ่านระบบเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะนั้น แน่นอนว่าผู้ลักลอบซึ่งเป็นผู้กระทำความผิดที่แท้จริงสมควรที่จะเป็นผู้กระทำความผิดและต้องรับโทษตามกฎหมาย แต่ในทางกลับกัน หากเจ้าของระบบเครือข่ายไร้สายได้ตั้งมาตรการป้องกันการเข้าถึงไว้ การกระทำความผิดก็จะเกิดได้ยาก ดังนั้น หากเจ้าของระบบเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงระบบเครือข่ายไร้สายไว้ จนเป็นเหตุให้มีการลักลอบเข้าถึงระบบเครือข่ายไร้สายในการกระทำความผิดก็สมควรที่จะต้องมีความรับผิดทางอาญาด้วย

---

(4) นำเข้าถึงระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)

มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

[38] พรเพชร วิชิตชลชัย, “คำอธิบาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550,” (กรุงเทพมหานคร : สำนักงานศาลยุติธรรม),หน้า 30

บทที่ 4
วิเคราะห์กรณีการลักลอบใช้บริการอินเทอร์เน็ตโดยมิชอบกับกฎหมายของต่างประเทศ

การลักลอบใช้บริการอินเทอร์เน็ตโดยมิชอบผ่านเครือข่ายไร้สายและการลักลอบใช้เครือข่ายไร้สายของผู้อื่นในการกระทำความผิดเป็นการกระทำที่พบได้บ่อยในต่างประเทศ เช่น ในประเทศสหรัฐอเมริกาและประเทศอังกฤษ ซึ่งในต่างประเทศล้วนมีกฎหมายที่ใช้บังคับเพื่อลงโทษกับการกระทำดังกล่าวเนื่องจากการกระทำดังกล่าวมีลักษณะที่กระทบต่อความเป็นส่วนตัว เศรษฐกิจ หรือในบางครั้งอาจจะกระทบถึงความสงบเรียบร้อยและความมั่นคงในสังคม ดังนั้น ในบทนี้จะได้กล่าวถึงการบัญญัติกฎหมายเพื่อป้องกันการลักลอบใช้บริการอินเทอร์เน็ตโดยมิชอบผ่านเครือข่ายไร้สายและการลักลอบใช้เครือข่ายไร้สายของผู้อื่นในการกระทำความผิด รวมทั้งความรับผิดทางกฎหมายในกรณีที่มีการกระทำดังกล่าว

4.1 การบัญญัติกฎหมายเพื่อป้องกันอาชญากรรมคอมพิวเตอร์และการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของประเทศสหรัฐอเมริกา

สหรัฐอเมริกาได้มีการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ขึ้นมาฉบับแรกเมื่อปี ค.ศ. 1984 ได้แก่ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 ซึ่งเป็นกฎหมายที่ออกมาเพื่อที่จะใช้แก้ปัญหาอาชญากรรมคอมพิวเตอร์โดยมีสาเหตุที่สำคัญประการหนึ่งในการออกกฎหมายฉบับนี้คือ การสูญเสียทางการเงินปีละหลายร้อยล้านเหรียญสหรัฐอเมริกา การบัญญัติกฎหมายฉบับนี้ สภาคองเกรสต้องใช้เวลาในการพิจารณาปัญหาต่างๆ เช่น การที่มีกฎหมายอาญาที่ใช้บังคับอยู่มากกว่า 40 ฉบับ สามารถนำมาใช้บังคับและครอบคลุมกับอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นได้เพียงใด ซึ่งในที่สุดสภาคองเกรสก็ตัดสินใจที่จะบัญญัติกฎหมายขึ้นมาใหม่ แทนการปรับปรุงกฎหมายที่ใช้บังคับอยู่ แต่ในขณะที่สภาคองเกรสกำลังพิจารณาปัญหาต่างๆอยู่ หลายมลรัฐในสหรัฐอเมริกาก็ได้บัญญัติกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์เป็นที่เรียบร้อยแล้ว[1]

---

[1]เลิศชาย สุธรรมพร, “อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย , 2541), หน้า 70

ภายหลังที่กฎหมายดังกล่าวได้ออกมาใช้บังคับแล้ว สหรัฐอเมริกาก็ยังคงเผชิญกับปัญหาจำนวนมาก เช่น ความเหมาะสมในการให้คำนิยามของคำว่า “อาชญากรรมคอมพิวเตอร์” (Computer Crime) การกระจัดกระจายของคำนิยามซึ่งน่าจะจัดอยู่ในมาตราเดียวกัน การจำกัดวงเพื่อป้องกันเฉพาะงานของรัฐไม่ขยายไปสู่ภาคเอกชน การขาดความชัดเจนในมูลค่าการฟ้องร้อง ความเหลื่อมล้ำของเขตอำนาจศาล และปัญหาเกี่ยวกับวิธีพิจารณาความ เช่น การหาพยานหลักฐานมาพิสูจน์ความผิดมีจำนวนน้อยมาก ทำให้ไม่สามารถนำผู้กระทำผิดมาลงโทษได้ ด้วยเหตุผลต่างๆเหล่านี้ นักกฎหมายและผู้ที่เกี่ยวข้องจึงได้เรียกร้องให้มีการปรับปรุงกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ในที่สุดก็มีการแก้ไขกฎหมายดังกล่าว วัตถุประสงค์ของการแก้ไขก็เพื่อที่จะเพิ่มประสิทธิภาพในการจัดการ และขจัดปัญหาต่างๆที่เกิดขึ้น แต่การแก้ไขก็ไม่ได้ครอบคลุมถึงการกระทำความผิดที่เกี่ยวกับการฉ้อฉลและการใช้คอมพิวเตอร์ในการกระทำความผิด

ต่อมาในปี ค.ศ. 1986 ได้มีการออกกฎหมายฉบับใหม่คือ The Computer Fraud and Abuse Act of 1986 โดยกฎหมายฉบับนี้ได้เปลี่ยนแปลงสาระสำคัญไปจากกฎหมายฉบับเดิม คือ

1. การเปลี่ยนเจตนาร้าย (Mens Rea) ตามมาตรา 1030 (a) (2) และ (a) (3) จาก “โดยรู้” (Knowingly) เป็น “โดยเจตนา” (Intentionally)
2. ขยายมาตราที่จะกำหนดคำนิยามในกฎหมาย

กล่าวโดยสรุปได้ว่า การบัญญัติกฎหมายฉบับนี้ ได้ตั้งความหวังว่าจะเพิ่มประสิทธิภาพของกฎหมายให้ดียิ่งขึ้น โดยเพิ่มการกระทำที่ต้องห้าม และการใช้กฎหมายที่เหลื่อมล้ำ โดยเน้นสาระสำคัญว่าการกระทำที่ถือว่าเป็นการกระทำความผิดจะต้องกระทำโดยเจตนา และใช้ภาษาที่ชัดเจนเพื่อขจัดการตีความ

อย่างไรก็ตาม กฎหมายฉบับนี้ที่มีการแก้ไขเพิ่มเติมอีกในปี ค.ศ. 1994, 1996 และในปี ค.ศ. 2001 ได้แก้ไขโดย USA Patriot Act ซึ่งได้เพิ่มขอบเขตและบทลงโทษของกฎหมายฉบับเดิมได้แก่[2]

---

[2] “Computer Fraud and Abuse Act,” [Online] Avaliable from : http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act (วันที่ 6 ธันวาคม 2551)

1. เพิ่มเติมบทกำหนดโทษในกรณีที่กระทำความผิดครั้งแรกจาก 5 ปีเป็น 10 ปี และการกระทำความผิดครั้งที่ 2 จาก 10 ปีเป็น 20 ปี
2. เป็นการยืนยันว่าผู้กระทำความผิดมีเจตนาที่จะกระทำความผิดโดยทั่วไปเท่านั้น ไม่ได้มีเจตนาที่จะกระทำความผิดหรือมีเจตนากระทำความผิดอื่นที่มีความเสียหายเกินกว่า 5,000 เหรียญสหรัฐอเมริกา
3. อนุญาตให้รวมความเสียหายจากคอมพิวเตอร์แตกต่างรายกันได้เป็นจำนวนถึง 5,000 เหรียญสหรัฐอเมริกา
4. ปรับปรุงบทลงโทษสำหรับผู้กระทำความผิดที่เกี่ยวข้องกับความเสียหายใดๆที่เกิดกับคอมพิวเตอร์ของรัฐบาลในการยุติธรรมทางอาญาหรือการทหาร
5. มีการรวมความเสียหายของคอมพิวเตอร์สัญชาติต่างประเทศที่เกี่ยวข้องกับการค้าขายระหว่างมลรัฐ
6. มีการรวมความผิดที่เกี่ยวกับมลรัฐให้ได้รับการพิจารณาความผิดก่อน และ
7. ขยายคำนิยามของความเสียหายเพื่อให้ชัดเจนว่ารวมถึงเวลาการตรวจสอบและการสนองตอบที่ต้องเสียไป

สำหรับเนื้อหาสาระของกฎหมายฉบับนี้โดยมากแล้วเน้นถึงการห้ามกระทำการใดๆ อันเป็นการเข้าถึงระบบในส่วนที่เกี่ยวข้องกับหน่วยงานรัฐบาลกลางของสหรัฐอเมริกาโดยปราศจากอำนาจ อีกทั้งกฎหมายกลางของสหรัฐอเมริกา (18 U.S.C.) ยังมีส่วนที่ได้บัญญัติถึงความผิดเกี่ยวกับการรบกวนหรือขัดขวางการสื่อสาร ความผิดฐานฉ้อฉลและกิจกรรมที่เกี่ยวเนื่องกับกลไกการเข้าถึง(ระบบเครือข่ายอินเทอร์เน็ต) รวมถึงกฎหมายที่เกี่ยวกับการเข้าถึงข้อมูลของคอมพิวเตอร์ที่ถูกเก็บไว้ในระบบคอมพิวเตอร์ ซึ่งแม้กฎหมายดังที่กล่าวนั้นส่วนใหญ่แล้วจะใช้บังคับเพื่อป้องกันผลประโยชน์ของสหรัฐอเมริกา แต่เมื่อเป็นกฎหมายของรัฐบาลกลางจึงมีความจำเป็นจะต้องพิจารณากับการกระทำอันเป็นการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายด้วยว่าจะเกี่ยวข้องกันหรือไม่เพียงใด

แต่อย่างไรก็ตาม การกระทำอันเป็นการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยทั่วไปแล้วจะเป็นการกระทำความผิดที่เอกชนกระทำต่อเอกชน ซึ่งกฎหมายที่บัญญัติความผิดทางอาญาระหว่างเอกชนกับเอกชนนั้นโดยมากจะบัญญัติไว้ในกฎหมายอาญาของแต่ละ

มลรัฐ ดังนั้นในกรณีนี้จึงจำเป็นที่จะต้องวิเคราะห์บทบัญญัติของกฎหมายอาญาของแต่ละมลรัฐที่เกี่ยวข้องด้วยดังที่จะปรากฏในหัวข้อต่อๆไป

4.2 ความรับผิดในการกระทำความผิดที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของประเทศสหรัฐอเมริกา

ความรับผิดในการกระทำความผิดเกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของประเทศสหรัฐอเมริกา จะต้องพิจารณาทั้งจากกฎหมายของรัฐบาลกลางในส่วนที่เกี่ยวกับ The Computer Fraud and Abuse Act of 1986 ซึ่งบัญญัติไว้ในกฎหมายของรัฐบาลกลางมาตรา 1030 (18 U.S.C. 1030 Fraud and related activity in connection with computers) ซึ่งเป็นส่วนที่เกี่ยวข้องกับการฉ้อฉลและกิจกรรมที่เกี่ยวเนื่องกับคอมพิวเตอร์และมาตรา 2701(18 U.S.C. 2701 Unlawful access to stored communications) ซึ่งเป็นส่วนที่เกี่ยวข้องกับการลักลอบเข้าถึงระบบโดยปราศจากอำนาจ รวมทั้งกฎหมายที่เกี่ยวกับการฉ้อฉลและกิจกรรมที่เกี่ยวเนื่องกับกลไกการเข้าถึง (ระบบเครือข่ายอินเทอร์เน็ต) ซึ่งบัญญัติไว้ในกฎหมายของรัฐบาลกลางมาตรา 1029 (18 U.S.C. 1029 Fraud and related activity in connection with access devices) ซึ่งเมื่อพิจารณากฎหมายกลางของสหรัฐอเมริกาแล้ว ในขั้นตอนต่อไปจะได้พิจารณากฎหมายอาญาของแต่ละมลรัฐเพื่ออธิบายถึงลักษณะการกระทำความผิดต่างๆเหล่านั้นต่อไป

4.2.1 ความผิดฐานลักลอบเข้าถึงระบบโดยปราศจากอำนาจ

ความผิดฐานลักลอบเข้าถึงระบบโดยปราศจากอำนาจเป็นความผิดชนิดหนึ่ง ซึ่งกฎหมายบัญญัติเป็นพิเศษไว้ใน The Computer Fraud and Abuse Act of 1986 ซึ่งเป็นส่วนหนึ่งของกฎหมายรัฐบาลกลางของสหรัฐอเมริกา มาตรา 1030 อันเป็นเรื่องฉ้อฉลและกิจกรรมที่เกี่ยวเนื่องกับคอมพิวเตอร์ (18 U.S.C. 1030 Fraud and related activity in connection with computers)[3] ซึ่งมีสาระสำคัญคือการกระทำของผู้กระทำความผิดโดยรู้อยู่แล้วหรือโดยเจตนาเพื่อที่จะเข้าถึงโดยปราศจากอำนาจหรือกระทำเกินอำนาจที่ตนมีอยู่ ดังรายละเอียดต่อไปนี้

---

[3](a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the

Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(a) ผู้ใด

(1) โดยรู้อยู่แล้วได้เข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือเข้าถึงระบบคอมพิวเตอร์เกินอำนาจที่ตนมีอยู่ และโดยการกระทำนั้นได้ไปซึ่งข้อมูลที่รัฐบาลสหรัฐอเมริกา มีคำสั่งของฝ่ายบริหารหรือกฎหมายลายลักษณ์อักษรที่ต้องการป้องกันการเปิดเผยโดยปราศจากอำนาจเพื่อความปลอดภัยของประเทศหรือความสัมพันธ์ระหว่างประเทศหรือเป็นข้อมูลใดๆที่เป็นความลับ ดังที่ได้กำหนดไว้ในย่อหน้า y ของมาตรา 11 ของพระราชบัญญัติพลังงานปรมาณู ค.ศ. 1954 (The Atomic Act of 1954) ซึ่งเป็นเหตุผลที่เชื่อได้ว่าข้อมูลที่ได้รับนั้นอาจถูกใช้สร้างความเสียหายต่อสหรัฐอเมริกาหรือเพื่อความได้เปรียบของชาติต่างประเทศโดยเจตนาที่จะสื่อสาร ส่ง ถ่ายทอด หรือทำให้เกิดการสื่อสาร ส่ง ถ่ายทอดหรือพยายามที่จะสื่อสาร

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;
shall be punished as provided in subsection (c) of this section.

[Online] Avaliable from : http://www.justice.gov/criminal/cybercrime/1030NEW.htm (10 ธันวาคม 2551)

ส่ง ถ่ายทอด หรือทำให้เกิดการสื่อสาร ส่ง ถ่ายทอดถึงบุคคลใดๆที่ไม่มีสิทธิจะได้รับข้อมูลนั้น หรือโดยเจตนาเก็บข้อมูลนั้นไว้และไม่สามารถส่งข้อมูลดังกล่าวไปยังเจ้าพนักงานหรือลูกจ้างของสหรัฐอเมริกาผู้มีสิทธิจะรับข้อมูลนั้น

(2) โดยเจตนาจะเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจที่ตนมีอยู่และโดยวิธีนั้นได้รับไปซึ่ง

(A) ข้อมูลทางการเงินของสถาบันการเงินหรือสถาบันที่ให้กู้ยืมตามที่ได้นิยามไว้ในมาตรา 1602 (n) ของบรรพ 15 หรือข้อมูลซึ่งเก็บไว้ในแฟ้มข้อมูลของผู้บริโภคซึ่งมีข้อความอย่างเดียวกับที่ได้บัญญัติไว้ในพระราชบัญญัติการรายงานเครดิต (The Fair Credit Reporting Act)

(B) ข้อมูลจากหน่วยงานใดๆของรัฐหรือตัวแทนของสหรัฐอเมริกา หรือ

(C) ข้อมูลจากคอมพิวเตอร์ที่มีการป้องกันไว้ถ้าการกระทำนั้นเกี่ยวข้องกับการ

ติดต่อสื่อสารระหว่างมลรัฐหรือการติดต่อสื่อสารระหว่างประเทศ

(3) โดยเจตนาเข้าถึงคอมพิวเตอร์ที่ไม่ได้มีไว้เพื่อการสาธารณะของหน่วยงานหรือตัวแทนของสหรัฐอเมริกาโดยปราศจากอำนาจ ซึ่งคอมพิวเตอร์ของหน่วยงานหรือตัวแทนนั้นมีไว้เพื่อใช้งานสำหรับรัฐบาลสหรัฐอเมริกาโดยเฉพาะ หรือในกรณีที่คอมพิวเตอร์นั้นไม่ได้ถูกใช้งานสำหรับรัฐบาลสหรัฐอเมริกาโดยเฉพาะ แต่ถูกใช้โดยหรือเพื่อรัฐบาลของสหรัฐอเมริกาและการกระทำดังกล่าวส่งผลกระทบต่อการใช้ของรัฐบาลของสหรัฐอเมริกาหรือการใช้งานสำหรับสหรัฐอเมริกา

(4) โดยรู้อยู่แล้วและโดยเจตนาที่จะฉ้อฉล, เข้าถึงคอมพิวเตอร์ที่มีการป้องกันไว้โดยปราศจากอำนาจหรือเกินกว่าขอบอำนาจที่มี และโดยการกระทำนั้นได้รับไปซึ่งสิ่งใดๆอันมีมูลค่า เว้นแต่วัตถุของการฉ้อฉลและสิ่งของที่ได้มานั้น รวมเฉพาะการใช้คอมพิวเตอร์และมูลค่าของการใช้ดังกล่าวไม่เกิน 5,000 เหรียญสหรัฐอเมริกาในช่วงเวลาหนึ่งปี

(5) (A)

(i) โดยรู้อยู่แล้วก่อให้เกิดการส่งโปรแกรม ข้อมูล รหัสหรือคำสั่งและผลของการกระทำนั้นมีเจตนาที่จะให้เกิดความเสียหายต่อคอมพิวเตอร์ที่มีการป้องกันไว้ทั้งนี้โดยปราศจากอำนาจ

(ii) เจตนาที่จะเข้าถึงคอมพิวเตอร์ที่มีการป้องกันไว้โดยปราศจากอำนาจและผลของการกระทำนั้นก่อให้เกิดความเสียหายโดยประมาทโดยรู้ตัว (Recklessness)[4] หรือ

(iii) เจตนาที่จะเข้าถึงคอมพิวเตอร์ที่มีการป้องกันไว้โดยปราศจากอำนาจและผลของการกระทำนั้นก่อให้เกิดความเสียหาย และ

(B) การกระทำดังที่ได้กล่าวไว้ใน อนุมาตรา (i), (ii) และ (iii) ของ (A) นั้นส่งผลให้ (หรือในกรณีที่เป็นการพยายามกระทำความผิดถ้าสำเร็จจะส่งผลให้)

(i) บุคคลหนึ่งคนหรือมากกว่านั้นมีความเสียหายในช่วงเวลา 1 ปี (และเพื่อวัตถุประสงค์ในการตรวจสอบ, ดำเนินคดีหรือกระบวนพิจารณาอย่างอื่นโดยสหรัฐอเมริกาเท่านั้น ซึ่งความเสียหายกระทบต่อคอมพิวเตอร์ที่มีการป้องกัน 1 เครื่องหรือมากกว่านั้น) รวมแล้วเป็นเงินรวมกันไม่ต่ำกว่า 5,000 เหรียญสหรัฐอเมริกา

(ii) แก้ไขเปลี่ยนแปลงหรือทำให้เสียหายหรือทำให้เสียหายซึ่งผลทดสอบทางการแพทย์, การวินิจฉัยโรคของแพทย์, การรักษาพยาบาลหรืออนามัยของบุคคลตั้งแต่ 1 คนหรือมากกว่าขึ้นไป

(iii) การทำให้ผู้ใดได้รับความเจ็บป่วยทางร่างกาย

(iv) การคุกคามต่อความปลอดภัยของสังคม หรือ

---

[4] ประมาทโดยรู้ตัว (Recklessness) เป็นสภาวะทางจิตอย่างหนึ่งที่ผู้กระทำไม่เพียงแต่ขาดความระมัดระวังเท่านั้น แต่ได้กระทำไปโดยเพิกเฉยไม่นำพาต่อเหตุการณ์ที่เกิดขึ้น กล่าวคือ ได้กระทำโดยรู้สึกอยู่แล้วว่าเป็นการเสี่ยงที่จะเกิดภัยแต่ยังขืนทำลง บางครั้งมีผู้เรียกลักษณะของสภาวะแห่งจิตเช่นนี้ว่า ประมาทโดยจงใจ (Advertent Negligence) คือ จงใจกระทำแต่ไม่แน่ว่าผลจะเกิดขึ้น หรือบางทีเรียกว่าเป็น Willfull Negligence ซึ่งในเรื่องนี้ศาลได้เคยวินิจฉัยไว้ในคดี R. V Bateman (1925) ว่าประมาทประเภทนี้ต้องถึงขนาดที่ลูกขุนเห็นว่าจะเพียงแต่ให้ใช้ค่าเสียหายกันยังไม่เพียงพอ เพราะเป็นความไม่นำพาต่อความปลอดภัยของผู้อื่นอันควรต้องรับผิดในทางอาญา

(v) ความเสียหายที่ส่งผลกระทบต่อระบบคอมพิวเตอร์ที่ใช้โดยหรือเพื่อรัฐบาลในส่วนบริหารงานยุติธรรม, การป้องกันภัยในประเทศหรือการรักษาความปลอดภัยภายในประเทศ

(6) โดยรู้อยู่แล้วและมีเจตนาฉ้อฉลถ่ายโอน (ตามที่ได้บัญญัติคำนิยามไว้ใน มาตรา 1029) รหัสลับหรือสารสนเทศที่คล้ายคลึงกันผ่านคอมพิวเตอร์ซึ่งได้มีการเข้าถึงระบบโดยปราศจากอำนาจ ถ้า

(A) แต่ละการถ่ายโอนส่งผลต่อภายในรัฐหรือธุรกิจของชาวต่างชาติ หรือ

(B) คอมพิวเตอร์แต่ละเครื่องถูกใช้โดยหรือเพื่อรัฐบาลของสหรัฐอเมริกา

(7) มีเจตนาที่จะบังคับขู่เข็ญจากบุคคลใดๆ เงินใดหรือสิ่งมีค่าอย่างอื่น, ส่งภายในระหว่างรัฐหรือธุรกิจของชาวต่างชาติซึ่งการสื่อสารใดๆที่ประกอบด้วยการคุกคามที่เป็นสาเหตุของความเสียหายต่อคอมพิวเตอร์ที่มีการป้องกันไว้

ซึ่งตามกฎหมายฉบับนี้ได้กำหนดคำนิยามเพื่อการใช้ การตีความกฎหมายที่ถูกต้องตามที่ปรากฏ ดังต่อไปนี้

(1) “คอมพิวเตอร์” หมายถึง เครื่องมือที่ใช้อิเล็กทรอนิกส์ แม่เหล็ก เคมีไฟฟ้าหรือเครื่องมืออย่างอื่นที่ใช้กระบวนการประมวลผลข้อมูลทางตรรกะด้วยความเร็วสูง คณิตศาสตร์ การทำงานเก็บข้อมูล และรวมถึงที่เก็บไว้เพื่อความสะดวกหรือเพื่อความสะดวกในการสื่อสารโดยทางตรงหรือระบบปฏิบัติการที่เชื่อมต่อกับเครื่องมือแต่ละตัว แต่ไม่รวมถึงเครื่องพิมพ์ดีดอัตโนมัติ เครื่องคิดเลขมือถือ หรือเครื่องมืออย่างอื่นที่คล้ายคลึงกัน

(2) “คอมพิวเตอร์ที่มีการป้องกัน” หมายถึง คอมพิวเตอร์ที่

(A) ใช้โดยเฉพาะในสถาบันการเงินหรือรัฐบาลสหรัฐอเมริกาหรือในกรณีที่คอมพิวเตอร์ไม่ได้ใช้ในกรณีดังกล่าวถูกใช้สำหรับสถาบันการเงินหรือรัฐบาลสหรัฐอเมริกาและมีผลเป็นความผิดในการใช้สำหรับสถาบันการเงินหรือรัฐบาลสหรัฐอเมริกา

(B) ซึ่งถูกใช้ในระหว่างรัฐหรือธุรกิจของชาวต่างชาติหรือการสื่อสาร รวมทั้งคอมพิวเตอร์ที่ตั้งอยู่นอกสหรัฐอเมริกาที่ถูกใช้ในการกระทำเกี่ยวกับระหว่างรัฐหรือธุรกิจของชาวต่างชาติหรือการสื่อสารของสหรัฐอเมริกา

เมื่อพิจารณามาตรา 1030 ประกอบกับคำนิยามแล้ว พบว่ากฎหมายมาตรานี้มีความประสงค์ที่จะป้องกันไม่ให้มีการบุกรุกเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจที่มีอยู่กับเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ใช้ในราชการของรัฐบาลของสหรัฐอเมริกาหรือหน่วยงานต่างๆของรัฐ รวมถึงสถาบันการเงิน ซึ่งในบางกรณีการเข้าถึงข้อมูลของรัฐหรือสถาบันการเงิน แม้คอมพิวเตอร์ที่เข้าถึงนั้นไม่ใช่คอมพิวเตอร์ที่มีการป้องกันก็เป็นความผิดแล้ว

เป็นที่น่าสังเกตว่า คำว่า “คอมพิวเตอร์ที่มีการป้องกัน” ในบทบัญญัติของกฎหมายมาตรา 1030 นี้มีความแตกต่างจากคำว่า “ระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ” ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เนื่องจากคำว่า “คอมพิวเตอร์ที่มีการป้องกัน” หมายถึงคอมพิวเตอร์ที่ใช้โดยเฉพาะในสถาบันการเงินหรือรัฐบาลสหรัฐอเมริกาหรือในกรณีที่คอมพิวเตอร์ไม่ได้ใช้ในกรณีดังกล่าวแต่ถูกใช้สำหรับสถาบันการเงินหรือรัฐบาลสหรัฐอเมริกาและมีผลเป็นความผิดในการใช้สำหรับสถาบันการเงินหรือรัฐบาลสหรัฐอเมริกา และอีกความหมายหนึ่งคือ คอมพิวเตอร์ที่ถูกใช้ในการค้าพาณิชย์หรือติดต่อสื่อสารระหว่างมลรัฐหรือระหว่างประเทศ รวมถึงคอมพิวเตอร์ที่ตั้งอยู่นอกประเทศสหรัฐอเมริกาซึ่งถูกใช้ในการค้าพาณิชย์หรือติดต่อสื่อสารระหว่างมลรัฐหรือระหว่างประเทศสหรัฐอเมริกา ซึ่งจะเห็นได้ว่าไม่ได้หมายรวมถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงแต่อย่างใด

ทั้งนี้เมื่อพิจารณาถึงวัตถุประสงค์ของกฎหมายมาตรา 1030 จะพบว่ามีวัตถุประสงค์หลักเพื่อป้องกันความมั่นคงปลอดภัยและรักษาความสงบเรียบร้อยของประเทศ โดยที่ไม่ได้มีเจตนาที่จะออกมาบังคับใช้กับการกระทำของเอกชนต่อเอกชน ซึ่งการกระทำอันเป็นการลักลอบเข้าถึงเครือข่ายไร้สาย (Wireless LAN : WLAN) เพื่อลักลอบใช้บริการอินเทอร์เน็ตผ่านสัญญาณไร้สายนั้นเป็นการกระทำที่เอกชนกระทำต่อระบบคอมพิวเตอร์ของเอกชนด้วยกัน ดังนั้น จึงเห็นได้ว่า การกระทำอันมีส่วนหนึ่งเป็นการลักลอบเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจนั้น ไม่อยู่ภายใต้บังคับของกฎหมายรัฐบาลกลาง มาตรา 1030 นี้

เมื่อพิจารณากฎหมายรัฐบาลกลางที่เกี่ยวข้องกับกฎหมายการสื่อสาร[5]เพิ่มเติมพบว่า การใช้คลื่นของสัญญาณไร้สาย ในส่วนของความชอบด้วยกฎหมายเกี่ยวกับกฎระเบียบของคณะกรรมการการสื่อสารของรัฐ (Federal Communications Commission : FCC) ส่วนที่ 15 ที่ว่าด้วยคลื่นที่ไม่มีลิขสิทธิ์ บุคคลใดก็ตามจึงสามารถใช้คลื่นสัญญาณไร้สายได้และการที่บุคคลมีเครื่องมือที่รับรองโดย FCC เช่น การ์ดที่รับสัญญาณไร้สาย ไม่มีบุคคลใดเป็นเจ้าของคลื่นสัญญาณไร้สาย ไม่มีใครได้รับสิทธิในการได้ใช้คลื่นสัญญาณไร้สายก่อนผู้อื่น ไม่มีกรรมสิทธิ์ในคลื่นนี้ ไม่มีสิ่งที่เรียกว่า การใช้สัญญาณไร้สายโดยปราศจากอำนาจ ตามที่สัญญาณไร้สายเป็นสิ่งสามัญที่ทุกคนมีสิทธิใช้โดยเท่าเทียมกัน การที่บุคคลใดเป็นเจ้าของ Access Point ไม่ได้หมายความว่าบุคคลนั้นเป็นเจ้าของคลื่นสัญญาณไร้สาย

การได้รับอนุญาตในการใช้ส่วนที่ 15 ในเรื่องของคลื่นสัญญาณไร้สายไม่เหมือนกับการอนุญาตให้ใช้เครือข่ายไร้สาย ถ้าเชื่อมต่อเข้าถึงระบบที่มีมาตรการป้องกัน จะมีอำนาจโดยชอบในการเข้าใช้คลื่นสัญญาณไร้สายแต่ไม่มีอำนาจในการเข้าถึงเครือข่าย เมื่อเจ้าของเครือข่ายป้องกัน Access Point จะไม่ใช่การจำกัดการเข้าใช้คลื่นสัญญาณไร้สาย เพียงแต่เป็นการปิดประตูในการเข้าถึง Access Point และไม่อนุญาตให้ใครเข้าใช้เครือข่ายไร้สาย ดังนั้น สิ่งที่ป้องกันคือเครือข่ายไร้สายไม่ใช่คลื่นสัญญาณไร้สาย

อย่างไรก็ตามมีกฎหมายของรัฐบาลกลางอีกมาตราหนึ่งที่เกี่ยวข้องกับการลักลอบเข้าถึงระบบโดยปราศจากอำนาจ แต่ในกรณีนี้เป็นการเข้าถึงข้อมูลการสื่อสารที่ถูกเก็บรักษาไว้ปรากฏในมาตรา 2701 (18 U.S.C. 2701 Unlawful Access to Stored Communications)[6] ซึ่งมีรายละเอียดดังต่อไปนี้

---

[5] Cybertelecom Federal Internet Law & Policy An Educational Project, “WiFi Theft / Piggy Backing :: Security,” [Online] Avaliable from : http://www.cybertelecom.org/broadband/wifisecurity.htm (15 มกราคม 2553)

[6](a) Offense.— Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(a) บทบัญญัติอันเป็นความผิด เว้นแต่ที่บัญญัติไว้ในอนุมาตรา (c) ของมาตรานี้ ผู้ใด

(1) โดยเจตนาเข้าถึงระบบโดยปราศจากอำนาจผ่านบริการการสื่อสารทางอิเล็กทรอนิกส์ซึ่งถูกกำหนดไว้ หรือ

(2) โดยเจตนาเข้าถึงระบบโดยกระทำเกินขอบอำนาจที่มี

โดยการกระทำนั้นได้รับ, เปลี่ยนแปลงหรือขัดขวางการเข้าถึงระบบโดยชอบในการสื่อสารแบบใช้สายหรือการสื่อสารทางอิเล็กทรอนิกส์**ในระหว่างที่ถูกเก็บรักษาด้วยวิธีทางอิเล็กทรอนิกส์**ในระบบสื่อสารนั้นๆ

ความผิดดังกล่าวนี้ถ้ากระทำโดยมีจุดประสงค์เพื่อความได้เปรียบทางเศรษฐกิจ, ทำให้เสียหายหรือทำลายหรือเพิ่มผลกำไรของเอกชนหรือเพื่อการกระทำความผิดอาญาต่อไปหรือการกระทำอันเป็นการละเมิดสิทธิในการฝ่าฝืนรัฐธรรมนูญหรือกฎหมายของสหรัฐอเมริกาหรือของมลรัฐ

ข้อยกเว้น ของอนุมาตรา (a) ของมาตรานี้ไม่รวมถึงการกระทำอันมีอำนาจทำได้ดังต่อไปนี้

(1) โดยบุคคลหรือผู้ใดที่มีอำนาจจัดการเกี่ยวกับการสื่อสารแบบใช้สายหรือการสื่อสารทางอิเล็กทรอนิกส์

(2) โดยผู้ใช้บริการของการสื่อสารนั้นๆ

---

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

Cornell University Law School, “U.S. Code Correction,” [Online] Avaliable from : http://www.law.cornell.edu/uscode/18/usc_sec_18_00002701----000-.html (8 ธันวาคม 2551)

(3) ในมาตรา 2703, 2704 และ 2518 ของบรรพนี้ (ซึ่งเกี่ยวกับผู้มีอำนาจเข้าถึงระบบได้โดยอำนาจตามกฎหมาย)

แท้ที่จริงแล้ววัตถุประสงค์ของกฎหมายมาตรา 2701 นี้บัญญัติขึ้นเพื่อคุ้มครองข้อมูลในอีเมล์ ทั้งนี้ก็เพื่อเป็นการป้องกันความลับ, ความครบถ้วนของบริการการสื่อสารซึ่งถูกเก็บรักษาไว้[7] ดังนั้น หากพิจารณามาตรา 2701 โดยเฉพาะในอนุมาตรา (a) (1) แล้วเห็นได้ว่า หากผู้ใดมีเจตนาลักลอบเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN : WLAN) ซึ่งกำลังสื่อสารข้อมูลกันอยู่ระหว่างอุปกรณ์ไร้สายกับ Access Point โดยการกระทำนั้นผู้กระทำได้รับ, เปลี่ยนแปลงหรือขัดขวางการเข้าถึงระบบโดยชอบในการสื่อสารทางอิเล็กทรอนิกส์ในระหว่างที่ข้อมูลถูกเก็บรักษาด้วยวิธีทางอิเล็กทรอนิกส์ในระบบสื่อสารนั้นๆ และการกระทำดังกล่าวนี้ผู้กระทำมีวัตถุประสงค์เพื่อความได้เปรียบทางเศรษฐกิจ, ทำให้เสียหายหรือทำลายหรือเพิ่มผลกำไรของเอกชนหรือเพื่อการกระทำความผิดอาญาต่อไปหรือการกระทำอันเป็นการละเมิดสิทธิในการฝ่าฝืนรัฐธรรมนูญหรือกฎหมายของสหรัฐอเมริกาหรือของมลรัฐ อาจจะถือได้ว่าเป็นการเข้าถึงระบบโดยไม่ชอบผ่านบริการสื่อสารทางอิเล็กทรอนิกส์ ตามความมุ่งหมายของมาตรานี้แล้ว ส่งผลให้ผู้บุกรุกอาจจะต้องรับโทษทางอาญา[8]

แต่อย่างไรก็ตาม หากพิจารณาลักษณะการลักลอบเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจในกรณีเอกชนกระทำต่อเอกชนเปรียบเทียบกับกฎหมายอาญาของบางมลรัฐในสหรัฐอเมริกาแล้ว พบว่า การกระทำลักษณะเช่นนี้ในบางมลรัฐบัญญัติให้เป็นความผิด เช่น ในมลรัฐอลาสก้า (Alaska) ซึ่งจะขอกล่าวรายละเอียดของกฎหมายที่บัญญัติห้ามการกระทำเช่นนี้ดังต่อไปนี้

---

[7] “Computer Crime & Intellectual Property Section,” [Online] Avaliable from : http://www.justice.gov/criminal/cybercrime/ccmanual/03ccma.html) (19 มีนาคม 2552)

[8] อย่างไรก็ดีนับแต่ที่กฎหมายฉบับนี้ได้ประกาศใช้ในปี ค.ศ. 1986 มีการดำเนินคดีภายใต้พระราชบัญญัติฉบับนี้น้อยมาก

มาตรา 11.46.740 ของบรรพ 11 กฎหมายอาญาแห่งมลรัฐอลาสก้า (Alaska)[9]

[9]AS 11.46.740. Criminal Use of Computer.

(a) A person commits the offense of criminal use of a computer if, having no right to do so or any reasonable ground to believe the person has such a right, the person knowingly accesses, causes to be accessed, or exceeds the person's authorized access to a computer, computer system, computer program, computer network, or any part of a computer system or network, and, as a result of or in the course of that access,

(1) obtains information concerning a person;

(2) introduces false information into a computer, computer system, computer program, or computer network with the intent to damage or enhance the data record or the financial reputation of a person;

(3) introduces false information into a computer, computer system, computer program, or computer network and, with criminal negligence, damages or enhances the data record or the financial reputation of a person;

(4) obtains proprietary information of another person;

(5) obtains information that is only available to the public for a fee;

(6) introduces instructions, a computer program, or other information that tampers with, disrupts, disables, or destroys a computer, computer system, computer program, computer network, or any part of a computer system or network; or

(7) encrypts or decrypts data.

(b) In this section, "proprietary information" means scientific, technical, or commercial information, including a design, process, procedure, customer list, supplier list, or customer records that the holder of the information has not made available to the public.

(c) Criminal use of a computer is a class C felony.

Alaska Legal Resource Center,

การกระทำความผิดอาญาเกี่ยวกับการใช้คอมพิวเตอร์

(a) บุคคลจะมีความผิดทางอาญาฐานใช้คอมพิวเตอร์กระทำอาชญากรรมถ้าบุคคลนั้นไม่มีสิทธิที่จะทำหรือพื้นฐานของความสมเหตุสมผลใดๆที่เชื่อว่าบุคคลมีสิทธิ บุคคลนั้นรู้อยู่แล้วได้เข้าไป, สืบเนื่องจากการเข้าไป หรือใช้สิทธิเกินขอบอำนาจที่ตนมีในการเข้าไปในคอมพิวเตอร์, ระบบคอมพิวเตอร์, โปรแกรมคอมพิวเตอร์, เครือข่ายคอมพิวเตอร์หรือส่วนหนึ่งส่วนใดของระบบหรือเครือข่ายคอมพิวเตอร์และการกระทำจากการเข้าไปนั้นส่งผลให้

(1) ได้รับข้อมูลเกี่ยวกับบุคคล
(2) นำข้อมูลเท็จเข้าถึงคอมพิวเตอร์, ระบบคอมพิวเตอร์, โปรแกรมคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์โดยมีเจตนาที่จะทำลายหรือปรับปรุงบันทึกข้อมูลหรือสถานะทางการเงินของบุคคล
(3) นำข้อมูลเท็จเข้าถึงคอมพิวเตอร์, ระบบคอมพิวเตอร์, โปรแกรมคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์โดยการกระทำเลินเล่อนั้นได้ทำลายหรือปรับปรุงบันทึกข้อมูลหรือสถานะทางการเงินของบุคคล
(4) ได้รับข้อมูลของบุคคลอื่น
(5) ได้รับข้อมูลที่มีไว้สำหรับสาธารณะเพื่อค่าธรรมเนียม
(6) นำคำสั่งวิธีการ, โปรแกรมคอมพิวเตอร์หรือข้อมูลอย่างอื่นซึ่งทำลาย , รบกวน, ทำให้เสียหายซึ่งคอมพิวเตอร์, ระบบคอมพิวเตอร์, โปรแกรมคอมพิวเตอร์, เครือข่ายคอมพิวเตอร์หรือส่วนหนึ่งส่วนใดของระบบหรือเครือข่ายคอมพิวเตอร์
(7) เปลี่ยนหรือทำลายรหัสข้อมูล

(b) ในมาตรานี้ “ข้อมูลของบุคคลอื่น” หมายถึง ข้อมูลเกี่ยวกับวิทยาศาสตร์ เทคนิคหรือข้อมูลทางการค้า รวมทั้งการออกแบบ กระบวนการ ขั้นตอน

[Online] Avaliable from :

http://touchngo.com/lglcntr/akstats/STATUTES/Title11/Chapter46/Section740.htm (วันที่ 10 ธันวาคม 2551)

รายชื่อลูกค้า รายชื่อผู้ส่งกระจายสินค้า หรือบันทึกลูกค้าซึ่งข้อมูลเช่นว่านี้ไม่ได้มีไว้เปิดเผยต่อประชาชน

(c) การกระทำความผิดนี้เป็น class c felony

การกระทำความผิดตามที่ได้กล่าวถึงข้างต้นนั้นได้เกิดเป็นคดีขึ้นแล้ว[10] เหตุการณ์นี้เกิดขึ้นในเมือง แอนโชเรจ (Anchorage) มลรัฐอลาสก้า (Alaska) ประเทศสหรัฐอเมริกา ซึ่งข้อเท็จจริงในคดีนี้มีอยู่ว่า มีชายผู้หนึ่ง คือ ไบรอัน แทนเนอร์ กำลังใช้สัญญาณไร้สายของห้องสมุดเพื่อเชื่อมต่อไปยังอินเทอร์เน็ต โดยทางเจ้าหน้าที่ห้องสมุดก็ได้แจ้งให้เจ้าหน้าที่ตำรวจทราบและเจ้าหน้าที่ตำรวจก็ได้เตือนให้ ไบรอัน แทนเนอร์ เลิกการกระทำนั้นเสียโดยบอกว่าการกระทำนั้นเป็นการใช้บริการอินเทอร์เน็ตของห้องสมุด แต่อย่างไรก็ตามในวันต่อมาตำรวจก็พบว่านายไบรอัน แทนเนอร์กระทำเช่นเดิมอีก จึงได้ยึดโน้ทบุ๊คของเขาเพื่อตรวจสอบว่าเขาอาจจะทำการดาวน์โหลด (Download) อะไรบางอย่าง ต่อมานายไบรอัน แทนเนอร์ ก็ได้รับสารภาพว่าเขามีเครื่องมือที่ใช้ในการดักฟังข้อมูลเพื่อใช้งานเครือข่ายไร้สายผ่านสัญญาณไร้สายที่ไม่ได้ตั้งมาตรการป้องกันไว้ได้ ซึ่งเมื่อเขาพบสัญญาณไร้สายของห้องสมุดนี้ เขาก็ได้ใช้โน้ทบุ๊คไปทำการลักลอบใช้สัญญาณของห้องสมุด ซึ่งนายไบรอัน แทนเนอร์ ก็ได้กล่าวต่อไปอีกว่า จริงๆแล้วที่บ้านของเขาก็สามารถใช้อินเทอร์เน็ตได้แต่พ่อแม่ของเขาไม่อนุญาตให้ใช้เล่นอินเทอร์เน็ตหลัง 3 ทุ่ม ในช่วงเวลากลางวันเขาจึงมาใช้สัญญาณไร้สายของห้องสมุด ซึ่งเจ้าหน้าที่ของห้องสมุดก็ได้ให้ปากคำต่อตำรวจว่า ในระหว่างนี้ห้องสมุดกำลังดำเนินการซ่อมแซมระบบเครือข่าย จึงเปิดระบบสัญญาณไร้สายไว้เพราะว่าจำเป็นต้องใช้ในการซ่อมแซมระบบ แต่โดยปกติแล้วจะปิดสัญญาณไร้สายเมื่อห้องสมุดปิดและโดยส่วนใหญ่ ไบรอัน แทนเนอร์ ก็จะมาใช้สัญญาณไร้สายในช่วงดังกล่าวเนื่องจากไม่มีผู้ใช้งานอื่นๆด้วย ทำให้สามารถใช้การได้เป็นอย่างดี

---

[10] “Palmer police seize computer of man using free wireless”

[Online] Avaliable from : http://torgo-x.livejournal.com/tag/libraries (วันที่ 10 ธันวาคม 2551)

4.2.2 ความผิดฐานลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย

การกระทำอันเป็นการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายที่ Access Point ของเครือข่ายไร้สาย (Wireless LAN : WLAN) ส่งออกมาโดยมีจุดประสงค์ที่จะเข้าถึงบริการอินเทอร์เน็ต ถือได้ว่าผู้กระทำการลักลอบนั้นได้รับผลประโยชน์จากการใช้บริการอินเทอร์เน็ตโดยที่ตนเองไม่ต้องเสียค่าใช้จ่าย การกระทำในลักษณะนี้เกี่ยวข้องโดยตรงกับการกระทำอันเป็นการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจ เนื่องจากการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีจุดประสงค์จะใช้บริการอินเทอร์เน็ตนั้น ผู้กระทำจะต้องผ่านเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN : WLAN) ของผู้อื่นเสียก่อน ซึ่งรายละเอียดของระบบการทำงานในส่วนนี้ได้กล่าวไว้แล้ว

ความผิดฐานลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย ในบางครั้งอาจเห็นได้ว่าเป็นการลักลอบใช้บริการรูปแบบหนึ่ง (Theft of Services) ซึ่งเมื่อพิจารณาเปรียบเทียบการกระทำเช่นนี้กับกฎหมายกลางของสหรัฐอเมริกาแล้ว พบว่ามีส่วนเกี่ยวข้องกับมาตรา 1029 อันเป็นบทบัญญัติที่เกี่ยวข้องกับการฉ้อฉลและกิจกรรมที่เกี่ยวเนื่องกับกลไกการเข้าถึง(ระบบเครือข่ายอินเทอร์เน็ต) (18 U.S.C. 1029 Fraud and Related Activity in connection with Access Devices)[11] ซึ่งมีรายละเอียดดังต่อไปนี้

---

[11] (a) Whoever—

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(a) ผู้ใด

---

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device;

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

Cornell University Law School, “U.S. Code Correction,” [Online] Avaliable from : http://www.law.cornell.edu/uscode/18/usc_sec_18_00001029----000-.html (8 ธันวาคม 2551)

(1) โดยรู้และมีเจตนาที่จะฉ้อฉล ผลิต ใช้หรือถ่ายโอนในสิ่งหนึ่งหรือหลายสิ่งซึ่งอุปกรณ์ที่ใช้เข้าถึงอันปลอมแปลง

(2) โดยรู้และมีเจตนาที่จะฉ้อฉล ถ่ายโอนหรือใช้สิ่งหนึ่งหรือหลายสิ่งซึ่งอุปกรณ์ที่ใช้เข้าถึงซึ่งปราศจากอำนาจในระหว่างระยะเวลา 1 ปีและการกระทำเช่นว่านั้นได้รับไปซึ่งมูลค่ารวมกันกว่า 1,000 เหรียญสหรัฐอเมริกาหรือกว่านั้น

(3) โดยรู้และมีเจตนาที่จะฉ้อฉล ครอบครอง อุปกรณ์ 15 ชิ้นหรือมากกว่านั้นซึ่งเป็นอุปกรณ์ที่ใช้เข้าถึงอันปลอมแปลงหรือปราศจากอำนาจ

(4) โดยรู้และมีเจตนาที่จะฉ้อฉล ผลิต ถ่ายโอน ควบคุมหรือป้องกันหรือครอบครองอุปกรณ์ซึ่งทำขึ้นเป็นเครื่องมือ

(5) โดยรู้และมีเจตนาที่จะฉ้อฉลอันส่งผลต่อการติดต่อทางธุรกิจ ด้วยอุปกรณ์ที่ใช้เข้าถึง 1 ชิ้นหรือมากกว่านั้นกับบุคคลอื่นเพื่อรับการชำระเงินหรือสิ่งอื่นซึ่งมีมูลค่าภายในระยะเวลา 1 ปีเป็นมูลค่ารวมกันจำนวนเท่ากับหรือมากกว่า 1,000 เหรียญสหรัฐอเมริกา

(6) โดยปราศจากอำนาจของผู้ออกอุปกรณ์ที่ใช้เข้าถึง โดยรู้และมีเจตนาที่จะฉ้อฉลบุคคลอื่นเพื่อวัตถุประสงค์

(A) เสนออุปกรณ์ที่ใช้เข้าถึง

(B) ขายสารสนเทศที่เกี่ยวข้องหรือคำร้องขอที่จะได้รับอุปกรณ์ที่ใช้เข้าถึง

(7) โดยรู้และมีเจตนาที่จะฉ้อฉล ใช้ ผลิต ถ่ายโอน ควบคุม ป้องกันหรือครอบครองเครื่องมือที่ใช้ในการโทรคมนาคมซึ่งถูกดัดแปลงหรือแก้ไขเพื่อให้ได้รับการบริการโทรคมนาคมที่ปราศจากอำนาจ

(8) โดยรู้และมีเจตนาที่จะฉ้อฉล ใช้ ผลิต ถ่ายโอน ควบคุมหรือป้องกันหรือครอบครองเครื่องตรวจรับ

(9) โดยรู้อยู่แล้วได้ใช้ ถ่ายโอน ควบคุมหรือป้องกันหรือครอบครองฮาร์ดแวร์หรือซอฟแวร์ที่ได้ถูกสร้างขึ้นเพื่อใส่หรือเปลี่ยนแปลงข้อมูลระบุชื่อของโทรคมนาคมร่วมกับหรือประกอบด้วยเครื่องมือโทรคมนาคมซึ่งเครื่องมือนั้นอาจถูกใช้ให้ได้รับบริการโทรคมนาคมโดยปราศจากอำนาจ หรือ

(10) โดยปราศจากอำนาจของระบบสมาชิกบัตรเครดิตหรือตัวแทน โดยรู้และมีเจตนาที่จะฉ้อฉลก่อให้เกิดหรือจัดการให้ผู้อื่นได้เป็นสมาชิกหรือตัวแทน

สำหรับการได้รับชำระเงิน โดยมีหลักฐานหรือบันทึกของการดำเนินธุรกิจหนึ่งครั้งหรือมากกว่านั้นที่กระทำโดยอุปกรณ์ที่ใช้เข้าถึง

ถ้าการกระทำนั้นส่งผลกระทบต่อระหว่างมลรัฐหรือธุรกิจของชาวต่างชาติ จะต้องถูกลงโทษตามที่บัญญัติไว้ในอนุมาตรา c

ส่วนคำนิยามนั้นจะปรากฏอยู่ในอนุมาตรา e ของมาตราเดียวกันซึ่งมีรายละเอียดดังต่อไปนี้

(a) ตามที่ได้ใช้ในมาตรานี้

(1) “อุปกรณ์ที่ใช้เข้าถึง” หมายความว่า บัตรใดๆ แผ่นโลหะ รหัส หมายเลขบัญชี หมายเลขรหัสอิเล็กทรอนิกส์ หมายเลขแสดงตัวเคลื่อนที่ หมายเลขแสดงตัวของบุคคลหรือบริการโทรคมนาคมอย่างอื่น อุปกรณ์หรือเครื่องมือที่ใช้ระบุชื่อหรือวิธีการอย่างอื่นของการเข้าบัญชีที่สามารถถูกใช้ได้โดยลำพังหรือร่วมกับอุปกรณ์ที่ใช้เข้าถึงอย่างอื่นเพื่อให้ได้รับเงิน สินค้า บริการหรือสิ่งมีค่าอย่างอื่นหรือที่สามารถใช้เริ่มการโอนกองทุน (นอกจากการโอนดั้งเดิมโดยเอกสารอันเป็นกระดาษ)

(2) “อุปกรณ์ที่ใช้เข้าถึงอันปลอมแปลง” หมายถึง อุปกรณ์ที่ใช้เข้าถึงใดๆซึ่งปลอม ไม่แท้ ถูกเปลี่ยนแปลงหรือส่วนประกอบซึ่งสามารถแสดงความเป็นตัวตนของอุปกรณ์ที่ใช้เข้าถึงหรืออุปกรณ์ที่ใช้เข้าถึงอันปลอมแปลง

(3) “อุปกรณ์ที่ใช้เข้าถึงโดยปราศจากอำนาจ” หมายถึง อุปกรณ์ที่ใช้เข้าถึงใดๆที่สูญหาย ถูกขโมย หมดอายุ ถูกเพิกถอน ถูกยกเลิกหรือได้รับมาจากการฉ้อฉล

(4) “บริการโทรคมนาคม” มีความหมายเช่นเดียวกับในพระราชบัญญัติโทรคมนาคม ค.ศ.1934 (Telecommunications Act of 1934) มาตรา 153 ซึ่งได้ให้ความหมายว่า การใช้โทรคมนาคมที่จ่ายค่าธรรมเนียมโดยตรงแก่สาธารณะโดยไม่จำต้องมีเครื่องอำนวยความสะดวกในการใช้โทรคมนาคมอย่างอื่น

เมื่อพิจารณามาตรา 1029 ดังกล่าวมาข้างต้นแล้วพบว่า กฎหมายมีความประสงค์ที่จะไม่ให้บุคคลใดๆทำการฉ้อฉลต่อกิจการระหว่างมลรัฐหรือธุรกิจของชาวต่างชาติ เป็นต้นว่า ห้าม

บุคคลลักลอบค้ารหัสหรือ หมายเลขบัตรเครดิตทางอินเทอร์เน็ตหรือใช้ซอฟท์แวร์หรือฮาร์ดแวร์ ในการผลิต หรือแพร่กระจายรหัสหรือหมายเลขบัตรเครดิต ซึ่งหากสามารถปรับการกระทำอันเป็นการลักลอบใช้สัญญาณไร้สายผ่านเครือข่ายไร้สายสู่การใช้บริการอินเทอร์เน็ตว่าเป็นการกระทำในลักษณะลักลอบใช้บริการโทรคมนาคมโดยปราศจากอำนาจตามมาตรา 1029 อนุมาตรา (a) (7) ก็ไม่สามารถจะปรับบทลงโทษได้ เพราะในบทกำหนดโทษตามมาตรา 1029 นี้ถูกกำหนดไว้ในตอนท้ายแล้วว่าจะต้องเป็นการกระทำที่กระทบต่อกิจการระหว่างมลรัฐและธุรกิจของชาวต่างชาติ

ดังนั้น เมื่อกฎหมายกลางของสหรัฐอเมริกามาตรา 1029 ไม่สามารถใช้บังคับกับการกระทำระหว่างเอกชนที่มีต่อเอกชนได้แล้ว จึงต้องพิจารณากับกฎหมายอาญาของแต่ละมลรัฐต่อไป ซึ่งพบว่ากฎหมายอาญาของบางมลรัฐบัญญัติให้การลักลอบใช้สัญญาณไร้สายเป็นความผิด เช่น ในกฎหมายอาญาของมลรัฐอิลลินอยส์ (Illinois) 720 ILCS 5/16F-3[12] ซึ่งมีรายละเอียดดังต่อไปนี้

---

[12](720 ILCS 5/16F-3)

Sec. 16F-3. Theft of wireless service.

(a) A person commits the offense of theft of wireless service if he or she intentionally obtains wireless service by the use of an unlawful wireless device or without the consent of the wireless service provider.

(b) Theft of wireless service is a Class A misdemeanor when the aggregate value of service obtained is less than $300 and a Class 4 felony when the aggregate value of service obtained is $300 or more. For a second or subsequent offense, or if the person convicted of the offense has been previously convicted of any similar crime in this or any other state or federal jurisdiction, theft of wireless service is a Class 2 felony.

Illinois General Assembly, “CRIMINAL OFFENSES (720 ILCS 5/) Criminal Code of 1961,” [Online] Avaliable from : http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=072000050HArt.+16F&ActID=1876&ChapterID=53&SeqStart=36700000&SeqEnd=37400000) (วันที่ 20 ธันวาคม 2551)

720 ILCS 5/16F-3

มาตรา 16F – 3 ลักลอบใช้บริการสัญญาณไร้สาย

(a) บุคคลใดกระทำความผิดโดยการลักลอบใช้บริการสัญญาณไร้สาย ถ้ามีเจตนาจะได้รับบริการสัญญาณไร้สายโดยการใช้อุปกรณ์ไร้สายที่ไม่ชอบด้วยกฎหมายหรือปราศจากความยินยอมของผู้ให้บริการสัญญาณไร้สาย

(b) การลักลอบใช้บริการสัญญาณไร้สายเป็นความผิดอาญาประเภทลหุโทษแบบ A ถ้าได้รับมูลค่าจากบริการนั้นรวมน้อยกว่า 300 เหรียญสหรัฐอเมริกา และเป็นความผิดอาญาระดับกลาง แบบ 4 ถ้าได้รับมูลค่าจากบริการนั้นรวม 300 เหรียญสหรัฐอเมริกาหรือมากกว่านั้น สำหรับการกระทำความผิดครั้งที่สองหรือมีความผิดอย่างอื่นอยู่แล้วหรือถ้าบุคคลนั้นถูกพิพากษาว่ามีความผิดมาแล้วในความผิดที่คล้ายคลึงกันในมลรัฐนี้หรือมลรัฐอื่นหรือตามกฎหมายกลางของสหรัฐอเมริกา การลักลอบใช้บริการสัญญาณไร้สายเป็นความผิดอาญาระดับกลาง แบบ 2

อย่างไรก็ดี ด้วยผลของกฎหมายฉบับนี้ ในมลรัฐอิลลินอยส์ได้เคยมีคดีเกี่ยวกับการลักลอบใช้บริการสัญญาณไร้สายเพื่อใช้บริการอินเทอร์เน็ต[13]แล้ว ดังมีรายละเอียดต่อไปนี้

ชายชาวอิลลินอยส์ ชื่อว่านายเดวิด คลูแช็ค ได้ถูกตำรวจจับในข้อหาเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยปราศจากความยินยอมของเจ้าของเครือข่ายในขณะที่เขากำลังใช้โน้ทบุ๊คในบริเวณที่เขาจอดรถซึ่งเป็นบริเวณที่มีสัญญาณไร้สายซึ่งถูกปล่อยจาก Access Point ขององค์กรไม่หวังผลกำไรโดยที่สัญญาณไร้สายนั้นไม่ได้มีการตั้งค่าความปลอดภัยไว้

ผลจากการกระทำดังกล่าวนายเดวิด คลูแช็ค ถูกปรับเงินจำนวน 250 เหรียญสหรัฐอเมริกาและถูกควบคุมความประพฤติโดยศาลเป็นเวลา 1 ปี ซึ่งในคดีนี้ อัยการรัฐแห่งเขตวินนีบาโก้ (Winnebago) คือนายพอล โลกลิ ได้กล่าวไว้ว่า การเข้าถึงเครือข่ายไร้สายของผู้อื่นผ่าน Access Point โดยปราศจากอำนาจ แม้ว่าเครือข่ายนั้นจะไม่ได้ตั้งค่าความปลอดภัยไว้ก็เป็น

---

[13] “Illinois WiFi freeloader fined US$250,” [Online] Avaliable from : http://arstechnica.com/old/content/2006/03/6447.ars (2 มกราคม 2552)

ความผิดตามกฎหมายอาญาของมลรัฐอิลลินอยส์ ซึ่งนายพอล โลกลิ ได้เตือนด้วยว่า หากผู้ใดยังคงฝ่าฝืนกระทำความผิดในลักษณะนี้อาจจะมีโอกาสถูกจำคุกหรือปรับ

สำหรับในมลรัฐอื่นพบว่ามีรายงานการกระทำความผิดฐานลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย ดังต่อไปนี้[14]

1. มลรัฐฟลอริด้า[15]

เจ้าหน้าที่ตำรวจเข้าจับกุมนายเบนจามิน สมิธ (Benjamin Smith) อายุ 41 ปี ในข้อหาใช้เครือข่ายอินเทอร์เน็ตไร้สายของผู้อื่นซึ่งเป็นความผิด third-degree felony เจ้าหน้าที่ตำรวจกล่าวหาว่านายเบนจามิน สมิธ ได้ใช้สัญญาณไร้สายจากบ้านนายริชาร์ด ดีน่อน (Richard Dinon) ซึ่งตามข้อเท็จจริงพบว่านายริชาร์ด ดีน่อนได้เตือนนายเบนจามิน สมิธแล้ว ในขณะที่เขานั่งอยู่ในรถยนต์และกำลังใช้โน้ทบุ๊ค

การกระทำดังกล่าวเป็นเรื่องใหม่ที่เกิดขึ้นในหน่วยงานบังคับกฎหมายของมลรัฐฟลอริด้า การใช้สัญญาณไร้สายของผู้อื่นในกรณีที่เป็นการใช้งานที่ไม่เป็นอันตรายอาจถือได้ว่าเป็นเรื่องธรรมดา แต่ผู้เชี่ยวชาญกล่าวว่าหากเป็นการใช้ที่เป็นเรื่องผิดกฎหมายก็จะตรวจสอบไม่ได้ เช่น การใช้เครือข่ายไร้สายของผู้อื่นในการส่งภาพอนาจาร, การขโมยข้อมูลบัตรเครดิตของผู้อื่น หรือการส่งข้อความข่มขู่ผู้อื่น เป็นต้น

2. มลรัฐมิชิแกน[16]

---

[14] Cybertelecom Federal Internet Law & Policy An Educational Project, “WiFi Theft / Piggy Backing :: Security,” [Online] Avaliable from : http://www.cybertelecom.org/broadband/wifisecurity.htm (15 มกราคม 2553)

[15] CBSNEWS, “Man Arrested For Stealing Wi-Fi,” [Online] Avaliable from : http://www.cbsnews.com/stories/2005/07/07/tech/main707361.shtml (10 สิงหาคม 2552)

[16] Foxnews, “MICHIGAN MAN FINED FOR USING COFFEE SHOP'S WI-FI NETWORK," [Online] Avaliable from :

นายแซม ปีเตอร์สัน (Sam Peterson) แห่งเมืองซีด้าร์ สปริง มลรัฐมิชิแกน ถูกปรับเงินจำนวน 400 เหรียญสหรัฐอเมริกาและต้องทำงานบริการสังคมจำนวน 40 ชั่วโมงจากการกระทำความผิดฐานเข้าถึงระบบอินเทอร์เน็ตผ่านเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของผู้อื่น โดยนายแซม ปีเตอร์สัน อยู่ภายนอกร้านกาแฟรียูเนี่ยน คาเฟ่และใช้โน้ทบุ๊คในการใช้บริการอินเทอร์เน็ตผ่านเว็บไซต์โดยอาศัยเครือข่ายไร้สายของร้านกาแฟรียูเนี่ยน คาเฟ่โดยที่นายแซม ปีเตอร์สันไม่ได้เข้าไปซื้อสินค้าในร้านกาแฟรียูเนี่ยนคาเฟ่แต่อย่างใด

นายแซม ปีเตอร์สัน กระทำเช่นนี้อยู่เป็นเวลาเกินกว่าสัปดาห์ จนกระทั่งมีผู้แจ้งให้เจ้าหน้าที่ตำรวจเข้าไปตรวจสอบเนื่องจากเห็นว่านายแซม ปีเตอร์สันนั่งอยู่ในรถหน้าร้านกาแฟรียูเนี่ยน คาเฟ่ทุกๆวัน เจ้าหน้าที่ตำรวจมิลาโนสกีจึงสอบถามว่าใช้การเชื่อมต่ออินเทอร์เน็ตจากที่ใด นายแซม ปีเตอร์สันก็กล่าวว่าใช้การเชื่อมต่อจากร้านกาแฟ

เจ้าหน้าที่ตำรวจมิลาโนสกี มีความสงสัยว่าการกระทำดังกล่าวของนายแซม ปีเตอร์สันเป็นการกระทำความผิดตามบทบัญญัติของกฎหมายมลรัฐหรือไม่ แต่เขารู้สึกเหมือนว่ากฎหมายกำลังถูกละเมิด จึงได้แจ้งให้ทางพนักงานอัยการดำเนินการ หลังจากนั้นอีกไม่กี่สัปดาห์ นายแซม ปีเตอร์สัน ก็ได้รับจดหมายจากสำนักงานอัยการเคนท์ เคาร์ตี้ (Kent Country) โดยในจดหมายกล่าวว่าเขาได้ถูกกล่าวหาว่าได้เข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยฉ้อฉล ซึ่งตามกฎหมายในปี ค.ศ. 1979 ซึ่งได้รับการแก้ไขในปี 2000 ได้บัญญัติขึ้นในการป้องกันภัยอันตรายที่เกิดขึ้นกับระบบอินเทอร์เน็ตและผู้ใช้เครือข่ายส่วนตัวจากแฮคเกอร์ซึ่งรวมถึงระบบเครือข่ายไร้สายด้วย นายลินน์ ฮอปกินส์ (Lynn Hopkins) อัยการผู้ช่วยของสำนักงานอัยการเคนท์ เคาร์ตี้ กล่าวว่าตามบทบัญญัติของกฎหมาย บุคคลที่เข้าถึงเครือข่ายของไร้สายผู้อื่นโดยได้รับอนุญาตหรือผู้ที่เข้าถึงเครือข่ายสาธารณะสามารถสันนิษฐานได้ว่าไม่เป็นความผิดแต่อย่างใด แต่หากเป็นการเข้าถึงเครือข่ายของบุคคลอื่นที่ไม่ใช่เครือข่ายสาธารณะก็จะเป็นความผิดตามกฎหมาย

---

http://www.foxnews.com/story/0,2933,276720,00.html (6 มีนาคม 2552)

3. มลรัฐวอชิงตัน[17]

เหตุเกิดที่เมืองแวนคูเวอร์ มลรัฐวอชิงตัน เมื่อนายอเล็กซานเดอร์ อิริค สมิธ (Alexander Eric Smith) วัย 20 ปี ได้ถูกจับกุมในความผิดฐานลักลอบใช้บริการ หลังจากที่เขาได้จอดรถที่หน้าร้านกาแฟและใช้เครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของร้านกาแฟเป็นเวลา 3 เดือน ทั้งๆที่เขาไม่ได้ซื้อสินค้าจากร้านกาแฟนั้นแต่อย่างใด

แต่อย่างไรก็ดีในบางมลรัฐ เช่น มลรัฐแคลิฟลอเนียร์[18]ได้กำหนดมาตรการที่เกี่ยวข้องกับการป้องกันการเข้าถึงเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันความปลอดภัย ซึ่งมีรายละเอียดบัญญัติอยู่ตามบทบัญญัติหมายเลข AB 2415 ที่บังคับให้เครื่องมือที่รวมถึง Access Point ที่ผลิตในวันที่หรือหลังวันที่ 1 ตุลาคม 2007 สำหรับใช้ในสำนักงานขนาดเล็ก, บ้านสำนักงาน (Home Office) หรือบ้านเรือน ซึ่งใช้คลื่นที่ไม่มีลิขสิทธิ์จะต้องแจ้งเตือนให้ผู้บริโภคทราบถึงวิธีการในการป้องกันการเชื่อมต่อเครือข่ายไร้สายและต้องมีเครื่องหมายเตือนหรือจัดการให้มีการป้องกันอื่นๆ รวมทั้งบังคับให้ต้องได้รับการแสดงความยินยอมจากผู้บริโภคก่อนใช้งานเครื่องมือนั้น

สำหรับการออกบทบัญญัติฉบับที่ AB 2415 นี้ อดีตผู้ว่าการมลรัฐแคลิฟลอเนียร์ อาร์โนด์ สวาเซเนคเกอร์ (Arnold Schwarzenegger) ได้ลงนามไว้ในวันที่ 30 กันยายน 2006 โดยอดีตผู้ว่าการรัฐกล่าวว่า “การช่วยเหลือป้องกันข้อมูลส่วนบุคคลทางอิเล็คทรอนิกส์เป็นเรื่องสำคัญมากตามที่การกระทำความผิดในลักษณะ Identity Theft (หรือที่เรียกว่า “การโจรกรรมอัตลักษณ์บุคคล) ได้เพิ่มมากขึ้น การออกกฎหมายฉบับนี้จะเป็นการช่วยให้ความรู้และป้องกันผู้บริโภคที่จะต้องเป็นเหยื่อของแฮคเกอร์และความอ่อนแอของเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกัน”

---

[17] Arstechnica, “WiFi freeloader arrested in Washington,” [Online] Avaliable from : http://arstechnica.com/old/content/2006/06/7111.ars) (10 ธันวาคม 2551)

[18] “AB 2415,” [Online] Avaliable from :

http://www.leginfo.ca.gov/pub/05-06/bill/asm/ab_2401-2450/ab_2415_bill_20060930_chaptered.html) (12 เมษายน 2553)

ซึ่งการขโมยข้อมูลส่วนบุคคลเป็นปัญหาที่กำลังเพิ่มขึ้นและทำความเสียหายแก่เหยื่อและองค์กรธุรกิจเป็นจำนวนกว่า 1 หมื่นล้านเหรียญสหรัฐอเมริการในทุกๆปี ผู้ซื้อที่นำไปใช้งานในบ้านและธุรกิจขนาดเล็กส่วนมากไม่ได้ตระหนักถึงความเสี่ยงที่จะเกิดขึ้นกับการใช้งานเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันไว้ น่าเสียดายที่ผู้บริโภคส่วนใหญ่ไม่ทราบว่าเป็นการอนุญาตให้ข้อมูลส่วนตัวของตนได้ถูกเข้าถึงโดยผู้ไม่มีสิทธิใช้งานที่ลักลอบเข้าถึงระบบเครือข่ายไร้สายผ่านเครื่องมือ

กฎหมายฉบับนี้ จึงเป็นการลดโอกาสที่จะเกิดการขโมยข้อมูลส่วนตัวสำหรับผู้บริโภคที่เป็นบ้านเรือนและธุรกิจขนาดเล็กโดยกำหนดให้ผู้ผลิตต้องมีการเตือนผู้บริโภคดังกล่าวข้างต้น

อนึ่ง ในบางมลรัฐ เช่น มลรัฐนิวยอร์ค[19]ได้กำหนดให้การเข้าถึงโดยปราศจากอำนาจในเครือข่ายคอมพิวเตอร์ของผู้อื่นต้องเป็นไปโดยที่ผู้กระทำ “ทราบ” ว่าการเข้าถึงเครือข่ายคอมพิวเตอร์ของผู้อื่นนั้นเป็นไปโดยปราศจากการอนุญาตโดยชัดแจ้งเพราะในคำนิยามศัพท์ในความผิดฐานเข้าถึงเครือข่ายคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจ ได้ให้นิยามคำว่า “โดยปราศจากอำนาจ” ไว้ว่าหมายถึง ใช้หรือเข้าถึงคอมพิวเตอร์, บริการคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์โดยปราศจากการอนุญาตของเจ้าของเครือข่ายหรือผู้ให้เช่าหรือจากบุคคลใดที่ได้รับสิทธิจากเจ้าของเครือข่ายหรือผู้ให้เช่า โดยผู้กระทำทราบว่าการใช้หรือการเข้าถึงของตนนั้นปราศจากการได้รับอนุญาตหรือภายหลังที่ได้รับคำเตือนอย่างชัดแจ้งว่าเป็นการกระทำโดยปราศจากอำนาจ

การพิสูจน์ว่าผู้กระทำใช้หรือเข้าถึงคอมพิวเตอร์, บริการคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ของผู้อื่นเมื่อเป็นการกระทำที่เลี่ยง, ฉ้อฉลหรือด้วยวิธีการใดๆที่หลีกเลี่ยงระบบป้องกันความปลอดภัยที่ติดตั้งในคอมพิวเตอร์หรือที่ผู้ที่มีอำนาจใช้งานได้กำหนดไว้จะเป็นพยานหลักฐานที่สันนิษฐานได้ว่าผู้กระทำนั้นได้ใช้หรือเข้าถึงคอมพิวเตอร์, บริการคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจ

---

[19] “Law of New York,” [Online] Avaliable from : http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$PEN156.00$$@TXPEN0156.00+&LIST=LAW+&BROWSER=BROWSER+&TOKEN=37356239+&TARGET=VIEW) (11 พฤศจิกายน 2553)

แม้ว่าการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของผู้อื่นที่เจ้าของไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้จะเป็นความผิดในหลายๆมลรัฐของประเทศสหรัฐอเมริกา แต่บางคน[20]เห็นว่าการกระทำดังกล่าวไม่ควรจะเป็นการกระทำที่ผิดกฎหมายเพราะการใช้เครือข่ายไร้สายของผู้อื่นไม่มีลักษณะเป็นการขโมยโดยเปรียบเทียบกับการฟังวิทยุหรือดูโทรทัศน์โดยใช้เสาอากาศถ้าสัญญาณไร้สายมายังบริเวณที่ผู้ต้องการใช้งานอยู่แล้วและสามารถเข้าใช้งานได้โดยไม่ต้องเจาะผ่านมาตรการป้องกันการเข้าถึง หรือเปรียบเทียบกับการที่เพื่อนบ้านได้รดน้ำต้นไม้โดยใช้สปริงเคอร์ (Sprinkler)และน้ำกระเด็นมายังสวนของบ้าน ดังนั้น การเข้าถึงเครือข่ายไร้สายของผู้อื่น จึงไม่ควรถือว่าเป็นการขโมย

อีกทั้ง การเข้าถึงเครือข่ายไร้สายนั้นเป็นการเข้าถึงโดยปราศจากอำนาจหรือไม่[21] บุคคลผู้ติ้งการใช้บริการอินเทอร์เน็ตจะรู้ได้อย่างไรว่าเป็นการเข้าถึงระบบเครือข่ายไร้สายโดยปราศจากอำนาจ มีเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงมากมายในหลายๆที่ นอกจากนี้สัญญาณไร้สายนั้น เครื่องมือไร้สายบางชิ้นสามารถเข้าถึงเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงโดยอัตโนมัติโดยที่บุคคลไม่ต้องทำอะไร และผู้เชี่ยวชาญหลายท่านเห็นว่า[22]การดำเนินคดีในลักษณะนี้ไม่เหมาะสม โดยโต้แย้งว่า ขึ้นอยู่กับเจ้าของเครือข่ายไม่ว่าเครือข่ายจะตั้งมาตรการป้องกันการเข้าถึงหรือไม่ได้ตั้งมาตรการป้องกัน ตามกฎหมายไม่ควรสันนิษฐานว่าผู้เข้าถึงเครือข่ายไร้สายผิด เป็นเจตนาของเจ้าของทรัพย์สิน ถ้าทรัพย์สินนั้นปิดอยู่ เจ้าของเครือข่ายไร้สายควรจะมีความรับผิดชอบในการแสดงเจตนาเกี่ยวกับการส่งสัญญาณไร้สาย เรื่องนี้เกี่ยวพันกับทฤษฎีกฎหมายกล่าวคือบุคคลมีภาระในการให้ข้อมูล (กล่าวคือ ข้อมูลที่ว่าเครือข่ายตั้งมาตรการป้องกันการเข้าถึงหรือไม่) ผู้ใช้อุปกรณ์ไร้สายสามารถตรวจสอบหาเครือข่าย

---

[20] Eric Bangeman, “The Ethics of "Stealing" a WiFi Connection,” [Online] Avaliable from : http://arstechnica.com/security/news/2008/01/the-ethics-of-stealing-a-wifi-connection.ars (25 ตุลาคม 2553)

[21] Cybertelecom Federal Internet Law & Policy An Educational Project, “WiFi Theft / Piggy Backing :: Security,” [Online] Avaliable from : http://www.cybertelecom.org/broadband/wifisecurity.htm (15 มกราคม 2553)

[22] Ibid,

ไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงได้แต่เป็นไปไม่ได้ที่ผู้ใช้จะตรวจสอบได้ว่าเป็นเครือข่ายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงจริงหรือไม่ หรือสัญญาณมาจากที่ใด ใครเป็นเจ้าของเครือข่ายและจะติดต่อกับเจ้าของเครือข่ายอย่างไร

แต่อย่างไรก็ตาม ความเห็นนี้ได้มีผู้โต้แย้งโดยเห็นว่าการลักลอบใช้อินเทอร์เน็ตผ่านเครือข่ายไร้สายของผู้อื่นที่เจ้าของไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ควรจะเป็นความผิด เพราะการเข้าถึงเครือข่ายไร้สายของผู้อื่นเป็นการใช้แบนวิดธ์ของเจ้าของเครือข่ายไร้สาย เช่น การที่ผู้ลักลอบใช้งานได้เชื่อมต่อระหว่างเครือข่ายสองเครือข่ายหรือใช้เล่นเกมส์ การกระทำนี้ในความเป็นจริงทำให้ประสิทธิภาพของการเชื่อมในระบบอินเทอร์เน็ตต่อลดลงเพราะมีจำนวนผู้เข้าใช้งานมากขึ้น ซึ่งความเห็นนี้ได้ถูกผู้ที่สนับสนุน (ว่าการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของผู้อื่นที่เจ้าของไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ไม่ควรเป็นความผิด) โต้แย้งว่าประเด็นในเรื่องแบนวิธด์ หากเจ้าของเครือข่ายไร้สายไม่ต้องการให้มีการลักลอบใช้งานเจ้าของเครือข่ายสามารถตั้งมาตรการป้องกันการเข้าถึงในการเชื่อมต่ออินเทอร์เน็ต จะส่งผลให้ผู้ลักลอบเข้าถึงระบบไม่สามารถเข้าได้ ผู้สนับสนุนกล่าวด้วยว่าผู้ลักลอบเข้าถึงระบบส่วนใหญ่เชื่อมต่อเข้าถึงอินเทอร์เน็ตเพียงเพื่อเชคอีเมล์หรือเชคข้อมูลไม่ใช่การใช้แบนวิดธ์ที่มากเกินไป

ท้ายที่สุด หากพิจารณาในเรื่องสถิติการลักลอบใช้อินเทอร์เน็ตผ่านเครือข่ายไร้สายของผู้อื่น พบว่ามีการรายงาน[23]ว่ากว่า 54% ของผู้ใช้คอมพิวเตอร์เคยละเมิดกฎหมาย โดยใช้สัญญาณไร้สายของผู้อื่นในการเข้าถึงอินเทอร์เน็ตโดยปราศจากการอนุญาต มีการคาดเดาว่าการลักลอบใช้สัญญาณไร้สายยังส่งผลให้ผู้ให้บริการอินเทอร์เน็ตได้รับค่าบริการที่ลดน้อยลงและทำให้ระบบการเชื่อมต่อของเพื่อนบ้านช้าลงโดยไม่ทราบว่าผู้ที่มาใช้งานเป็นใคร

---

[23]Sophos Press Release, “Wi-Fi piggybacking widespread, Sophos research reveals,” [Online] Avaliable from :

http://www.sophos.com/pressoffice/news/articles/2007/11/wi-fi.html (3 กันยายน 2553)

4.2.3 ความผิดเกี่ยวกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์เพื่อกระทำความผิด

ระบบเครือข่ายไร้สายที่เจ้าของเครือข่ายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ ผู้ลักลอบสามารถนำอุปกรณ์ไร้สายเข้าเชื่อมต่อกับระบบเครือข่ายไร้สายได้โดยง่าย ซึ่งการลักลอบเข้าถึงระบบเครือข่ายไร้สายนี้อาจเป็นการกระทำที่ผู้ลักลอบต้องการกระทำความผิดโดยอาศัยเครือข่ายไร้สายของผู้อื่น ซึ่งการกระทำความผิดที่เคยเกิดขึ้นนั้นมี 2 กรณี[24]ไม่ว่าจะเป็นการลักลอบใช้เครือข่ายไร้สายของผู้อื่นในการดาวน์โหลดภาพอนาจารเด็กหรือการลักลอบดาวน์โหลดหรือเผยแพร่สินค้าอันเป็นการละเมิดลิขสิทธิ์ ซึ่งการกระทำความผิดในแต่ละลักษณะนั้นมีรายละเอียดดังต่อไปนี้

1. การลักลอบใช้ระบบเครือข่ายไร้สายของผู้อื่นในการส่งภาพอนาจาร[25]

เหตุการณ์นี้เกิดขึ้นในมลรัฐฟลอริด้า เจ้าหน้าที่ได้เข้าจับกุมนางแคนดิซ มิลเล่อร์ (Candice Miller) หลังจากก่อนหน้านี้บุกเข้าจับกุมผิดบ้าน โดยพนักงานสืบสวนได้เข้าจับกุมในบ้านของนายเทด เดวิส (Ted Davis) ซึ่งเป็นเพื่อนบ้านของนางแคนดิซ มิลเล่อร์ เพราะสงสัยว่ามีการส่งภาพอนาจารเด็กบนเครือข่ายอินเทอร์เน็ตแต่กลับกลายเป็นว่าบ้านของนายเทด เดวิสนั้นใช้เครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงระบบอินเทอร์เน็ตไว้

นายเทด เดวิสกล่าวว่านางแคนดิซ มิลเล่อร์ ได้ลักลอบใช้เครือข่ายไร้สายที่ไม่ได้ตั้งค่าป้องกันของตนในการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ต ซึ่งเจ้าหน้าที่ได้แจ้งให้ทราบว่านางแคนดิซ มิลเล่อร์ ได้ใช้ระบบเครือข่ายไร้สายดังกล่าวในการส่งภาพอนาจารของตนกับลูกทั้งสองคนของเธอ ซึ่งการส่งภาพอนาจารบนระบบอินเทอร์เน็ตเป็นความผิดตามกฎหมาย

---

[24] "6 Reasons Why You Should Secure Your Unsecured Wi-Fi Wireless Network, What Can Happen, What To Do (such as porn)," [Online] Avaliable from : http://hubpages.com/hub/6-Reasons-Why-You-Should-Secure-Your-Wi-Fi-Network) (31 กรกฎาคม 2553)

[25] "Unsecured internet connection leads to law enforcement raid," [Online] Avaliable from : http://www.winknews.com/Local-Florida/2010-10-07/Unsecure-internet-connection-leads-to-law-enforcement-raid (2 กุมภาพันธ์ 2553)

อีกคดีหนึ่งเกิดที่เมืองอาร์ลิงตั้น เคอร์ตี้[26] (Arlington County) เจ้าหน้าที่ตำรวจบุกเข้าไปใน อพาร์ทเมนต์พร้อมหมายจับเพื่อต้องการจับผู้ต้องสงสัยในความผิดเกี่ยวกับการร่วมเพศกับเด็กซึ่งได้นำภาพอนาจารของเด็กเข้าถึงระบบออนไลน์ แต่ปรากฏว่าการเข้าจับกุมล้มเหลวเพราะเมื่อบุกเข้าไปก็พบแต่หญิงชราซึ่งสามารถสรุปได้ทันทีว่าไม่ใช่ผู้กระทำความผิดนี้

ปัญหามีอยู่ว่าเครือข่ายไร้สายของหญิงชรานี้ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ ทำให้สัญญาณไร้สายที่กระจายออกไป 10 ช่วงตึกและส่งผลให้ผู้ใดก็ตามสามารถเข้ามาใช้เครือข่ายไร้สายของหญิงชราได้ เจ้าหน้าที่กล่าวว่าบางทีผู้ที่กระทำความผิดคงเป็นเพื่อนบ้านของหญิงชราที่อยู่ในละแวกนี้

2. การลักลอบดาวน์โหลดหรือเผยแพร่สินค้าอันเป็นการละเมิดลิขสิทธิ์

เหตุการณ์นี้เกิดขึ้นในเมืองดูลูท มลรัฐมินเนโซต้า[27] นางแจมมี่ โทมัส วัย 30 ปีหรือผู้ที่ใช้นามแฝงว่า “Tereastarr” ได้กระทำละเมิดลิขสิทธิ์เพลงโดยการดาวน์โหลดและแชร์ไฟล์เพลง โดยคดีนี้คณะกรรมการสิ่งบันทึกเสียงแห่งอเมริกา (The Recording Industry Association of America : RIAA) ได้ดำเนินการฟ้องร้องเรียกค่าเสียหายเกือบ 1 ล้านเหรียญสหรัฐฯ

ตามคำให้การในคดีนี้ นามแฝง “Tereastarr” ได้ถูกใช้แทนตัวนางแจมมี่ โทมัส ในเว็บไซต์ Match.com, ชื่ออีเมล์และการเข้าถึงระบบในเว็บไซต์อื่นๆ คณะกรรมการสิ่งบันทึกเสียงแห่งอเมริกา (RIAA) ได้ชี้ให้เห็นว่านามแฝงนี้ได้ใช้ในการแชร์ไฟล์เพลงดิจิทัลจำนวน 1,700 บทเพลง พยานของคณะกรรมการสิ่งบันทึกเสียงแห่งอเมริกา (RIAA) ได้ให้การว่า หมายเลข IP Address ที่ทางผู้ให้บริการอินเทอร์เน็ตได้จัดสรรให้แก่นางแจมมี่ โทมัสเป็นแหล่งเดียวกับที่ใช้ในการแชร์ไฟล์เพลงบนเครือข่ายอินเทอร์เน็ต

---

[26] Jamie Stockwell, “WiFi Turns Internet Into Hideout for Criminals,” [Online] Avaliable from : http://www.washingtonpost.com/wp-dyn/content/article/2007/02/10/AR2007021001457.html (1 พฤษภาคม 2553)

[27] “Capitol v. Thomas,” [Online] Avaliable from : http://en.wikipedia.org/wiki/Capitol_v._Thomas และ “RIAA Rips Defendant in Nation’s First Filesharing Jury Trial,” [Online] Avaliable from : http://www.wired.com/threatlevel/2007/10/riaa-rips-defen (1 พฤษภาคม 2553)

ต่อมาทนายจำเลย (ทนายของนางแจมมี่ โทมัส) ได้ถามค้านพยานโจทก์ว่า การที่จำเลยเป็นเจ้าของเครือข่ายไร้สายที่ไม่ได้ตั้งค่าป้องกันไว้เป็นไปได้หรือไม่ ที่จะมีผู้อื่นเข้ามาใช้งานเครือข่ายไร้สายนี้ พยานโจทก์ตอบว่า เป็นไปได้ ซึ่งคดีดังกล่าวนี้ยังอยู่ในระหว่างการพิจารณาคดีของศาล

สำหรับคดีที่เสร็จการพิจารณาของศาลแล้วคือคดีที่เกิดขึ้นในมลรัฐแคลิฟลอเนียร์[28] คือ คดีที่บริษัท เวอร์จิ้น เรคคอร์ด อเมริกา จำกัด (Virgin Records America, INC.,) เป็นโจทก์ยื่นฟ้องนางแทมมี่ มาร์สัน (Tammie Marson) โดยกล่าวหาว่าจำเลยได้ดาวน์โหลดเพลงในระบบอินเทอร์เน็ตโดยละเมิดลิขสิทธิ์ของโจทก์ ซึ่งคดีนี้ศาลได้พิพากษายกฟ้องโดยไม่ตัดสิทธิในการฟ้องคดีใหม่[29] โดยศาลเห็นว่าจำเลยสามารถพิสูจน์ได้ว่าจำเลยซึ่งเป็นเจ้าของเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ไม่ใช่เป็นผู้ที่ใช้งานเครือข่ายไร้สายนั้นแต่เพียงผู้เดียว โดยที่จำเลยมีอาชีพเป็นครูสอนเชียร์ลีดเดอร์ มักจะมีผู้รับการฝึกเชียร์ลีดเดอร์มาที่บ้านของจำเลยเป็นจำนวนกว่าร้อยคนซึ่งอาจจะเป็นผู้ใดก็ได้ที่ได้ทำการดาวน์โหลดเพลงโดยละเมิดลิขสิทธิ์

คดีต่อมาเป็นคดีที่เกิดขึ้นในมลรัฐโอกลาโฮมา[30] (Oklahoma) คณะกรรมการสิ่งบันทึกเสียงแห่งอเมริกา (RIAA) ได้ฟ้องคดีนางเด็บบี้ ฟอสเตอร์ (Debbie Foster) ในความผิดฐาน

---

[28] “RIAA Drops Open WiFi Case – Virgin v. Marson,” [Online] Avaliable from : http://daledietrich.com/imedia/riaa-drops-open-wifi-case-virgin-v-marson และ “RIAA Discontinued Case in California, Virgin v. Marson,” [Online] Avaliable from : http://recordingindustryvspeople.blogspot.com/2006/07/riaa-discontinued-case-in-california.html (23 ตุลาคม 2553)

[29] [Online] Avaliable from : http://www.ilrweb.com/viewILRPDFfull.asp?filename=virgin_marson_stiporder (23 ตุลาคม 2553)

[30] Ken Fisher, “The RIAA, IP addresses, and evidence,” [Online] Avaliable from : http://arstechnica.com/old/content/2006/08/7416.ars และ Eric Bangeman, “RIAA loses in file sharing case,” [Online] Avaliable from : http://arstechnica.com/old/content/2006/07/7257.ars (25 ตุลาคม 2553)

ละเมิดลิขสิทธิ์ RIAA เรียกร้องให้นางฟอสเตอร์ชำระเงินจำนวน 5,000 เหรียญสหรัฐอเมริกาในการประนีประนอมยอมความ แต่นางฟอสเตอร์ต้องการต่อสู้คดีเพราะตนไม่ได้ทำและเห็นว่าการที่อาศัย IP Address เป็นพยานหลักฐานในการพิสูจน์ว่าเจ้าของเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้เป็นผู้กระทำความผิดในการละเมิดลิขสิทธิ์นั้นไม่เพียงพอเพราะ IP Address ไม่ใช่แผนที่ในการบอกว่าใครเป็นผู้ใช้งานเครือข่ายไร้สาย

ข้อเท็จจริงในคดีนี้มีอยู่ว่านางฟอสเตอร์และสามีได้หย่าขาดจากกันหลังจากที่นางถูกฟ้องคดีและก่อนการฟ้องคดีนั้น นางไม่ได้เป็นผู้ใช้คอมพิวเตอร์เลย ในขณะที่สามีของนางเป็นผู้ใช้คอมพิวเตอร์ แสดงให้เห็นว่าในขณะที่ทั้งสองยังไม่ได้หย่าขาดจากกันก็มีเฉพาะแต่สามีของนางฟอสเตอร์ที่ใช้คอมพิวเตอรื ทำให้มีข้อต่อสู้ว่าบุคคลอื่นที่อาศัยอยู่ในบ้านอาจจะเป็นผู้กระทำความผิดก็ได้ สุดท้าย RIAA ได้ถอนฟ้องคดีนี้

ส่วนคดีสุดท้ายเป็นคดีที่เกิดขึ้นในเมืองบลู แอช มลรัฐโอไฮโอ[31] (BLUE ASH, Ohio) บริษัท พาราเม้าส์ จำกัด (Paramount) ซึ่งเป็นผู้จัดจำหน่ายภาพยนตร์เรื่อง “Coach Carter” ได้ฟ้องคดีนายรัสเซล ลี (Russell Lee) ในความผิดฐานรับไว้ซึ่งภาพยนตร์ที่ผิดกฎหมายและอัพโหลดภาพยนต์เข้าถึงระบบออนไลน์ที่เรียกว่า “eDonkey” แต่เขาได้ปฏิเสธว่าไม่ได้เป็นผู้กระทำความผิดดังกล่าว

นายลี ได้กล่าวอ้างว่า ระบบเครือข่ายไร้สายของตนไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ในขณะมีการกระทำความผิด ดังนั้น บุคคลใดก็ตามสามารถมาจอดรถบริเวณใกล้บ้านหรือหน้าบ้านของเขาเพื่อลักลอบเข้าถึงระบบเครือข่ายไร้สายได้ นายลีกล่าวว่าการไม่ตั้งมาตรกรป้องกันการเข้าถึงเครือข่ายไร้สาย จะส่งผลให้มีผู้ลักลอบเข้าใช้งานเครือข่ายไร้สายได้ ดังนั้นเจ้าของเครือข่ายไร้สายควรต้องตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายเพื่อจะได้ไม่เกิดปัญหาอย่างตน

สำหรับการอาศัยระบบเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ของผู้อื่นในการเข้าถึงระบบอินเทอร์เน็ตเพื่อกระทำความผิดอาจจะมีได้อีกหลายกรณี เช่น การลักลอบ

---

[31] New5, “Movie Company Files Federal Piracy Suit Against Tri-State Man,” [Online] Avaliable from :

http://www.wlwt.com/health/5520020/detail.html (25 ธันวาคม 2553)

เข้าถึงระบบเครือข่ายไร้สายของผู้อื่นเพื่อใช้บริการอินเทอร์เน็ตโดยมีวัตถุประสงค์ในการประจานหรือทำให้ผู้อื่นได้รับความเสื่อมเสีย[32] (Cyber-Bullying)

อย่างไรก็ดี มีการตระหนักว่าการปล่อยให้เครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้อาจจะเป็นอันตรายต่อระบบข้อมูลที่เก็บรักษาไว้ในระบบคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายไร้สาย ทำให้ในบางเมือง เช่น เมืองเวสท์เชสเตอร์ เคาร์ตี้ มลรัฐนิวยอร์ก (Westchester County, New York) ได้ออกกฎหมายโดยกำหนดให้องค์กรธุรกิจในเมืองจะต้องทำการป้องกันระบบเครือข่ายไร้สายของตน ถ้าระบบเครือข่ายไร้สายนั้นได้ถูกใช้สำหรับการเข้าถึงข้อมูลทางการเงินของลูกค้า[33]

การออกกฎหมายดังกล่าวนี้ นายแอนดริว สปาโน่ (Andrew Spano) ผู้บริหารเมืองเวสเชสเตอร์ เคาร์ตี้ ให้ความเห็นว่าจะเป็นการลดปัญหา Identity Theft (บางครั้งเรียกว่า “การโจรกรรมอัตลักษณ์บุคคล) ยกตัวอย่างเช่น การขโมยข้อมูลจากฐานลูกค้าบัตรเครดิตไปใช้ในการทำธุรกรรมอื่น ทั้งนี้จากการตรวจสอบพบว่าในการสำรวจเครือข่ายไร้สายของเมืองเวสเชสเตอร์เคาร์ตี้ภายใน 20 นาทีพบเครือข่ายไร้สายถึง 248 แห่งและครึ่งหนึ่งเป็นเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ จึงเป็นที่มาของการออกกฎหมายในการให้เจ้าขององค์กรธุรกิจไร้

---

[32] “Suicide of Megan Meier,” [Online] Avaliable from : http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier และ “N.J. Student Secretly Taped Having Sex in Dorm Posted Suicide Plunge Message on Facebook,” [Online] Avaliable from : http://www.foxnews.com/us/2010/09/29/rutgers-students-accused-secretly-taping-sex-dorm-posting-video-online (10 มกราคม 2554)

[33]“New law requires some businesses to secure their WiFi networks,” [Online] Avaliable from : http://arstechnica.com/old/content/2006/04/6647.ars (10 มกราคม 2554)

สายมีมาตรการป้องกันเครือข่ายไร้สายของตนและกำหนดให้เจ้าขององค์กรธุรกิจมีหน้าที่ต้องเตือนลูกค้าผู้ใช้บริการในการเข้าถึงเครือข่ายไร้สายที่ไม่ได้ตั้งมาตราการป้องกันการเข้าถึงไว้[34]

การลักลอบใช้บริการอินเทอร์เน็ตโดยการเข้าถึงระบบคอมพิวเตอร์ผ่านเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ มีความเห็น[35]ว่าควรเป็นความผิดในฐานที่เจ้าของระบบคอมพิวเตอร์ประมาทเลินเล่ออย่างร้ายแรง (Gross Negligence)[36] เนื่องจากการไม่ได้ตั้งมาตรการป้องกันไว้ส่งผลให้ผู้ลักลอบสามารถกระทำความผิดอื่นได้ เช่น ดาวน์โหลดภาพอนาจารเด็ก ฉ้อโกง ลักลอบข้อมูลบัตรเครดิต ส่งผลให้ผู้เสียหายจากการกระทำความผิด (เหยื่อ) สามารถฟ้องร้องเรียกค่าเสียหายจากเจ้าของเครือข่ายไร้สายได้

และสุดท้ายหากเจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้จนเป็นเหตุให้มีผู้ลักลอบเข้าถึงเครือข่ายไร้สายนั้นในการกระทำความผิด เจ้าของเครือข่ายไร้สายที่ละเลย

---

[34] รายละเอียดของกฎหมายฉบับนี้ปรากฏใน “Westchester's Wi-Fi Legislation,” [Online] Avaliable from :

http://consumer.westchestergov.com/index.php?option=com_content&view=article&id=2600&Itemid=100081 (2 มกราคม 2554)

[35] “Unsecured wireless owners being sued by victims,” [Online] Avaliable from :

http://www.dba-oracle.com/oracle_news/2005_7_29_wireless_owners_sued.htm (วันที่ 10 กันยายน 2552)

[36] ประมาทเลินเล่ออย่างร้ายแรง หมายความว่า เป็นการกระทำโดยตั้งใจเพิกเฉยที่จะใช้ความระมัดระวัง ซึ่งการกระทำนั้นอาจจะส่งผลเสียหายต่อชีวิต ร่างกาย ทรัพย์สินของบุคคลอื่นได้ เมื่อเทียบกับการกระทำโดยประมาทเลินเล่ออย่างทั่วไปแล้ว การกระทำโดยประมาทเลินเล่ออย่างร้ายแรงมีลักษณะที่ประมาทเลินเล่อมากกว่า

“The Free Dictionary By Farlex,” [Online] Avaliable from : http://legal-dictionary.thefreedictionary.com/Gross+negligence (24 มิถุนายน 2553)

ต่อการป้องกันดังกล่าวอาจต้องมีความรับผิดตามกฎหมาย ซึ่งมีรายงานว่า[37]ศาลอาญาของประเทศเยอรมันได้ตัดสินว่าผู้ใช้บริการอินเทอร์เน็ตมีหน้าที่ต้องป้องกันระบบเครือข่ายไร้สายของตนโดยการตั้งรหัสผ่านเพื่อเป็นการป้องกันมิให้บุคคลที่ไม่มีอำนาจในการเข้าใช้งานได้เข้ามาดาวน์โหลดข้อมูลโดยไม่ชอบด้วยกฎหมาย

ผู้ใช้บริการอินเทอร์เน็ตจะถูกปรับเป็นเงินจำนวน 100 ยูโร (126 เหรียญสหรัฐ) ถ้ามีผู้ลักลอบใช้บริการอินเทอร์เน็ตในการดาวน์โหลดเพลงหรือไฟล์อื่นๆโดยผิดกฎหมาย โดยศาลกล่าวว่า ผู้ใช้บริการอินเทอร์เน็ตมีหน้าที่จะต้องตรวจสอบว่าระบบเครือข่ายไร้สายของตนมีการป้องกันที่เพียงพอในการป้องกันอันตรายจากการที่มีผู้ลักลอบใช้เครือข่ายไร้สายของตนในการกระทำความผิดเกี่ยวกับการละเมิดลิขสิทธิ์

แต่อย่างไรก็ตาม ศาลได้จำกัดคำตัดสินไว้ว่า ผู้ใช้บริการมีเพียงหน้าที่ที่จะต้องติดตั้งรหัสผ่านสำหรับการเข้าใช้งานเครือข่ายไร้สายเฉพาะการติดตั้งเครือข่ายไร้สายในครั้งแรกเท่านั้น แต่ไม่ได้วางหลักเกณฑ์ให้ผู้ใช้บริการจะต้องมีหน้าที่ในการพัฒนามาตรการป้องกันระบบเครือข่ายไร้สายของตนอย่างต่อเนื่อง

คำตัดสินนี้มีขึ้นหลังจากที่นักดนตรี (ผู้ที่ศาลไม่ได้ระบุว่าเป็นใคร) ได้ฟ้องผู้ใช้บริการอินเทอร์เน็ตรายหนึ่งว่าเครือข่ายไร้สายของผู้ใช้บริการรายนี้ได้ถูกใช้ในการดาวน์โหลดเพลงโดยไม่ชอบด้วยกฎหมายภายในเครือข่ายอินเทอร์เน็ต แต่ในคดีนี้ผู้ใช้บริการพิสูจน์ได้ว่าในขณะเกิดการกระทำผิดเขาได้อยู่ระหว่างการท่องเที่ยว แต่ศาลก็ยังคงตัดสินคดีโดยวางหลักว่าผู้ใช้บริการอินเทอร์เน็ตมีหน้าที่ที่จะต้องป้องกันไม่ให้มีผู้ลักลอบใช้งาน

---

[37] “German court orders wireless passwords for all Users can be fined if a third party takes advantage of an open connection,” [Online] Avaliable from : http://www.msnbc.msn.com/id/37107291/ns/technology_and_science-security (12 มกราคม 2554)

4.3 การบัญญัติกฎหมายเพื่อป้องกันการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของประเทศอังกฤษ

เมื่อกล่าวถึงอาชญากรรมคอมพิวเตอร์ โดยมากแล้วการกระทำอันเป็นอาชญากรรมคอมพิวเตอร์มักจะเป็นการกระทำต่อระบบคอมพิวเตอร์มากกว่าใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ซึ่งเดิมในประเทศอังกฤษอาชญากรรมคอมพิวเตอร์ เช่น การเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจไม่เป็นความความผิดตามกฎหมายอาญา โดยเปรียบเทียบกับการกระทำความผิดฐานบุกรุก (Trespass) และความผิดเกี่ยวกับทรัพย์สิน (Theft)[38] การกระทำนั้นเพียงแต่ทำให้ผู้กระทำต้องรับผิดทางแพ่งเท่านั้น ต่อมาด้วยความเจริญของระบบคอมพิวเตอร์ทำให้ระบบคอมพิวเตอร์เผยแพร่ออกไปมาก ซึ่งแน่นอนว่าการกระทำความผิดอันเป็นอาชญากรรมคอมพิวเตอร์ย่อมมากขึ้นตามไปด้วย ส่งผลให้ประเทศอังกฤษมีความจำเป็นต้องออกกฎหมายเพื่อยับยั้ง ขัดขวาง การกระทำเหล่านั้นเพื่อที่จะรักษาความปลอดภัยของระบบคอมพิวเตอร์ ทั้งในด้านเกี่ยวกับความสมบูรณ์ของระบบ ความลับของระบบและความสามารถใช้งานได้ซึ่งนับว่าการออกกฎหมายในลักษณะนี้เป็นสิ่งที่ผิดปกติ (Anomaly) เพราะแม้แต่การบุกรุกที่เป็นการกระทำทางกายภาพโดยเข้าไปในบ้านของบุคคลยังไม่เป็นความผิดทางอาญา แต่การบุกรุกเข้าไปทางอิเล็กทรอนิกส์ในการเข้าสู่ระบบประมวลผลของผู้อื่นกลับเป็นความผิดทางอาญา

ประเทศอังกฤษจึงได้บัญญัติกฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ขึ้นเป็นฉบับแรก คือ The Computer Misuse Act 1990 เมื่อวันที่ 29 สิงหาคม ค.ศ. 1990 ซึ่งบัญญัติให้การเข้าถึงระบบประมวลผลของคอมพิวเตอร์โดยปราศจากอำนาจเป็นความผิดอาญา โดยไม่จำกัดบุคคลที่กระทำการเข้าถึง ไม่ว่าจะเป็นพนักงานหรือลูกจ้างที่ไม่มีอำนาจ หรือบุคคลภายนอกใดๆก็ตาม ซึ่งการบัญญัติให้การเข้าถึงโดยปราศจากอำนาจเป็นความผิดอาญาตามหลักกฎหมายดังกล่าวนี้

ต่อมาเมื่อมีการใช้กฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (The Computer Misuse Act 1990) ไปสักระยะหนึ่งแล้ว ก็ได้มีการแก้ไขปรับปรุงกฎหมายฉบับ

---

[38] เลิศชาย สุธรรมพร, “อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย , 2541), หน้า 70

ดังกล่าว[39] โดยบัญญัติบทแก้ไขปรับปรุงไว้ในพระราชบัญญัติตำรวจและการยุติธรรม ค.ศ. 2006 (The Police and Justice Act 2006) ดังมีรายละเอียดที่จะได้กล่าวถึงในหัวข้อต่อๆไป

ในส่วนที่เกี่ยวข้องกับการป้องกันการลักลอบใช้บริการระบบเครือข่ายคอมพิวเตอร์นั้น ประเทศอังกฤษได้บัญญัติพระราชบัญญัติว่าด้วยการสื่อสาร ค.ศ. 2003 (The Communication Act 2003) โดยมีรายละเอียดตามที่จะกล่าวถึงในหัวข้อต่อๆไป

4.4 ความรับผิดในการกระทำความผิดที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของประเทศอังกฤษ

ตามบทบัญญัติใน The Computer Misuse Act 1990[40] ได้บัญญัติความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ ซึ่งการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจนั้น แบ่งออกเป็น 3 ประการด้วยกันคือ

1. ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access)

2. ความผิดฐานเข้าถึงโดยปราศจากอำนาจโดยมีเจตนาที่จะกระทำ หรือเพื่อความสะดวกในการกระทำความผิดอื่น (Unauthorized Access with Intent to Commit or Facilitate Commission of Further Offence)

3. ความผิดฐานทำให้เสียหายซึ่งระบบปฏิบัติการของคอมพิวเตอร์

---

[39] Wikipedia, the free encyclopedia, “Computer Misuse Act 1990,” [Online] Avaliable from :

http://en.wikipedia.org/wiki/Computer_Misuse_Act_1990 (20 ธันวาคม 2551)

[40] Office of Public Sector Information, “Computer Misuse Act 1990,” [Online] Avaliable from :

http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm (20 ธันวาคม 2551)

ความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจตามข้อ 1และข้อ 2 จะนำมาวิเคราะห์กับการกระทำอันเป็นการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) รวมไปถึงการกระทำที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์เพื่อกระทำความผิด

ส่วนลักษณะความผิดในข้อที่ 3 ส่วนใหญ่จะเป็นการกระทำอันมีลักษณะเป็นการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมีความประสงค์จะทำความเสียหายต่อเครื่องที่ตนบุกรุกเข้าไป เช่น การปล่อยไวรัส หรือ หนอนคอมพิวเตอร์ (Worm) เป็นต้น

ส่วนความรับผิดทางอาญาที่เกี่ยวกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สาย จะพิจารณาตามพระราชบัญญัติว่าด้วยการสื่อสาร ค.ศ. 2003 (The Communication Act 2003)

4.4.1 ความผิดฐานลักลอบเข้าถึงระบบโดยปราศจากอำนาจ

ตามบทบัญญัติใน The Computer Misuse Act 1990 ประกอบกับบทบัญญัติบางส่วนที่ได้แก้ไขเพิ่มเติมใน พระราชบัญญัติตำรวจและการยุติธรรม ค.ศ. 2006 (The Police and Justice Act 2006)[41] มีการบัญญัติความผิดฐานเข้าถึงโดยปราศจากอำนาจไว้ในมาตรา 1 โดยบัญญัติว่า[42]

---

[41] Office of Public Sector Information, “The Police and Justice Act 2006,” [Online] Avaliable from : http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060048_en.pdf) (20 ธันวาคม 2551)

[42] (1)A person is guilty of an offence if—

(a)he causes a computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secured ;

(b)the access he intends to secure or to enable to be secured is unauthorised; and

(1) บุคคลจะมีความผิดถ้า

(a) บุคคลได้กระทำการให้คอมพิวเตอร์[43]แสดงผล หรือแสดงการกระทำใดๆโดยจงใจที่จะผ่านสิ่งป้องกันที่มีไว้เพื่อกันการเข้าถึงระบบ และได้ทำการผ่านสิ่ง

(c)he knows at the time when he causes the computer to perform the function that that is the case.

(2)The intent a person has to have to commit an offence under this section need not be directed at—

(a)any particular program or data;

(b)a program or data of any particular kind; or

(c)a program or data held in any particular computer.

[Online] Avaliable from :

http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences) (13 มีนาคม 2552)

[43] The Computer Misuse Act 1990 ไม่ได้ให้คำนิยามของคำว่าคอมพิวเตอร์ไว้ เนื่องจากเกรงว่าคำนิยามจะล้าสมัยเมื่อเทคโนโลยีมีการพัฒนาไป แต่ศาลอังกฤษในคดี DPP v McKeown, DPP v Jones ได้เคยให้คำนิยามคอมพิวเตอร์ไว้ว่าเป็นเครื่องมือที่ใช้การเก็บ, การดำเนินการและการกู้ข้อมูล (อ้างใน www.parliament.uk, “House of Lord : Judgments -- Director of Public Prosecutions v. McKeown Director of Public Prosecutions v. Jones”)

[Online] Avaliable from :

http://www.publications.parliament.uk/pa/ld199697/ldjudgmt/jd970220/mcke01.htm (16 มิถุนายน 2553)

ป้องกันเช่นว่านั้นเข้าถึงโปรแกรมคอมพิวเตอร์ใดๆหรือสารสนเทศที่เก็บไว้ในคอมพิวเตอร์หรือทำให้สามารถเข้าถึงคอมพิวเตอร์ที่มีระบบป้องกันอยู่

(b) การผ่านสิ่งป้องกันเข้าไปในระบบหรือทำให้สามารถเข้าถึงคอมพิวเตอร์ที่มีระบบป้องกันนั้น เป็นการกระทำโดยปราศจากอำนาจ และ

(c) บุคคลนั้นได้รู้ขณะที่กระทำอยู่แล้วว่า เขาได้กระทำการอันเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานนั้นปราศจากอำนาจ

(2) เจตนาของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำที่เป็น

(a) โปรแกรมพิเศษเฉพาะเจาะจงใดๆหรือข้อมูล หรือ

(b) โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆหรือ

(c) โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ

ตามบทบัญญัติดังกล่าวเห็นได้ว่า เป็นบทบัญญัติพื้นฐานที่ใช้กับการเข้าถึงโดยปราศจากอำนาจที่ไม่สลับซับซ้อนเท่าใดนัก โดยเน้นการกระทำที่เป็นความผิดต้องเป็นการทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ แต่ไม่รวมถึงการกระทำทางกายภาพที่กระทำต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ อย่างไรก็ตามความผิดตามมาตรานี้ รวมถึงการสั่งให้คอมพิวเตอร์แสดงการทำงานโดยระยะไกล (Remote) ด้วยและไม่คำนึงถึงผลของการกระทำ เช่น ไม่คำนึงว่าผู้กระทำจะประสบความสำเร็จในการเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลหรือไม่ หรือผู้กระทำจะประสบความสำเร็จในการที่จะผ่านมาตรการป้องกันความปลอดภัยหรือไม่ กล่าวคือ แค่เป็นเพียงการพยายามก็เป็นความผิดแล้ว[44]และไม่ต้องพิจารณาว่าการเข้าถึงระบบการทำงานของคอมพิวเตอร์โดยปราศจากอำนาจนั้น ผู้กระทำจะตั้งใจทำอันตรายหรือไม่ อนึ่ง หากมีการกระทำความผิดตามมาตรานี้เกิดขึ้นจะต้องถูกนำไปพิจารณายังศาลแขวง (Magistrate's courts)

---

[44] “Computer Misuse Act Explained” [Online] Avaliable from :

http://knol.google.com/k/norman-creaney/computer-misuse-act-explained/1hzaxtdr9c09g/8#) (14 สิงหาคม 2553)

ขอบเขตของการกระทำความผิดตามมาตรานี้ค่อนข้างเป็นไปอย่างบททั่วไป[45] ยกตัวอย่างเช่นในคดีของเอลลิสและพนักงานอัยการ (Ellis v DPP) มีรายละเอียดของคดีว่า[46] จำเลยเป็นอดีตนักศึกษาของมหาวิทยาลัย ซึ่งมีข้อกำหนดว่านักศึกษาที่จบการศึกษาแล้วสามารถใช้ได้เฉพาะคอมพิวเตอร์ที่เข้าถึงระบบได้แบบเปิด (open-access university computers) เท่านั้น แต่อย่างไรก็ดีมีอยู่ 3 ครั้งด้วยกันที่จำเลยได้ใช้คอมพิวเตอร์ที่ไม่ใช่ประเภทที่เข้าถึงระบบได้แบบเปิด (non-access university computers) เพื่อใช้อินเทอร์เน็ต ซึ่งการที่จำเลยเข้าใช้งานคอมพิวเตอร์ประเภทนี้ได้เพราะว่าผู้ใช้งานคนก่อนยังไม่ได้ออกจากระบบ แม้ว่าจำเลยจะไม่มีรหัสผ่านในการเข้าถึงระบบคอมพิวเตอร์ จำเลยอ้างว่าจำเลยไม่ได้กระทำความผิดและได้เปรียบเทียบกับการอ่านหนังสือพิมพ์ที่ผู้อื่นทิ้งไว้ แต่อย่างไรก็ตาม การพิพากษาลงโทษจำเลยโดยอาศัยมาตรานี้ได้รับการสนับสนุนโดยถือว่าการกระทำของจำเลยเป็นการกระทำที่มีผลให้คอมพิวเตอร์ทำหน้าที่โดยมีเจตนาผ่านสิ่งที่ป้องกันไว้เพื่อเข้าถึงโปรแกรมใดๆหรือข้อมูลในคอมพิวเตอร์ โดยไม่มีอำนาจในการกระทำเช่นนั้นซึ่งจำเลยควรตระหนักอยู่แล้วว่าจำเลยไม่มีอำนาจ

ดังนั้น หากเปรียบเทียบกับกรณีการเข้าถึงระบบคอมพิวเตอร์เพื่อใช้บริการอินเทอร์เน็ตโดยผ่านการใช้สัญญาณไร้สายที่ Access Point แพร่สัญญาณออกมา จะเห็นได้ว่าเป็นการกระทำที่ครบองค์ประกอบของความผิดตามที่มาตรา 1 ได้บัญญัติไว้ เพราะว่าการกระทำดังกล่าวเป็นการกระทำที่ผู้กระทำจงใจเข้าถึงระบบคอมพิวเตอร์ ซึ่งการลักลอบเข้าถึงระบบคอมพิวเตอร์เพื่อใช้บริการอินเทอร์เน็ต ผู้กระทำจะลักลอบใช้อุปกรณ์ไร้สายจับสัญญาณไร้สายที่

---

[45] "Law in the Last Mile : Sharing Internet Access Through WiFi," [Online] Avaliable from : http://www.law.ed.ac.uk/ahrc/script-ed/vol6-2/macsithigh.asp) (12 กันยายน 2553)

[46] "Principles of Cybercrime โดย Jonathan Clough," [Online] Avaliable from : http://books.google.co.th/books?id=JVPnCqEuTksC&pg=PR17&lpg=PR17&dq=Ellis+v+DPP+2001&source=bl&ots=GLQbPIbXII&sig=2Et8vue1XTwb2r1mBScccb29hZM&hl=th&ei=B6UuTfDBI8KxrAeSz4S6Cg&sa=X&oi=book_result&ct=result&resnum=9&ved=0CFAQ6AEwCA#v=onepage&q=Ellis%20v%20DPP%202001&f=false) (30 มิถุนายน2553)

Access Point แพร่ออกมา เมื่อดักจับสัญญาณไร้สายดังกล่าวได้ ผู้ลักลอบก็จะสามารถเข้าถึงระบบคอมพิวเตอร์เพื่อใช้บริการอินเทอร์เน็ตได้ต่อไปเนื่องจาก Access Point ซึ่งเป็นอุปกรณ์ชิ้นหนึ่งของระบบคอมพิวเตอร์ทำหน้าที่เชื่อมต่อระหว่างอุปกรณ์ไร้สายกับระบบอินเทอร์เน็ต (ผ่านทางสายโทรศัพท์) จึงมีลักษณะเป็นการกระทำที่ผู้กระทำได้จงใจให้คอมพิวเตอร์ (ในที่นี้คือ Access Point) แสดงการทำงานใดๆ (ในที่นี้คือทำหน้าที่ส่งข้อมูลจากอุปกรณ์ไร้สายที่ผู้ลักลอบนำมาเชื่อมต่อไปยังระบบอินเทอร์เน็ต) แต่อย่างไรก็ตามจะต้องเป็นการผ่านเข้าถึงระบบคอมพิวเตอร์ที่ได้มีการตั้งค่าป้องกันการเข้าถึงเอาไว้ด้วย ทำให้การเข้าถึงระบบคอมพิวเตอร์เพื่อใช้บริการอินเทอร์เน็ตผ่านสัญญาณไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงของผู้อื่นนั้น ผู้กระทำจะไม่มีความผิดตามมาตรานี้แต่อย่างใด

4.4.2 ความผิดฐานลักลอบใช้บริการอินเทอร์เน็ตผ่านสัญญาณไร้สาย

ในบางครั้งการลักลอบผ่านเข้ามายังระบบเครือข่ายไร้สาย (Wireless LAN) กระทำไปโดยที่ผู้กระทำมีเจตนาจะใช้ประโยชน์จากการที่ระบบเครือข่ายไร้สาย (Wireless LAN) นั้นทำการสื่อสารอยู่กับระบบอินเทอร์เน็ตโดยเมื่อผู้ลักลอบสามารถเชื่อมต่อกับระบบเครือข่ายไร้สาย (Wireless LAN) เป็นที่เรียบร้อยแล้วก็จะสามารถใช้บริการอินเทอร์เน็ตได้โดยไม่ต้องเสียค่าใช้จ่ายแต่อย่างใด ซึ่งในกรณีนี้มีความเห็นที่สนับสนุนว่า[47] การกระทำดังกล่าวไม่ใช่ความผิดในการเข้าถึงเครือข่ายไร้สายของเจ้าของเครือข่าย เป็นแต่เพียงความผิดในลักษณะเป็นการที่ผู้กระทำเข้าใช้งานอินเทอร์เน็ตได้โดยหลบเลี่ยงการชำระค่าบริการเท่านั้น

ในประเทศอังกฤษนั้นมีการบัญญัติห้ามมิให้มีการกระทำอันเป็นการได้รับบริการการสื่อสารทางอิเล็กทรอนิกส์โดยไม่ชอบซึ่งบัญญัติไว้เป็นพระราชบัญญัติการสื่อสาร ปี ค.ศ. 2003

---

[47] “Law in the Last Mile: Sharing Internet Access Through WiFi,”

[Online] Avaliable from :

http://www.law.ed.ac.uk/ahrc/script-ed/vol6-2/macsithigh.asp (12 กันยายน 2553)

(Communications Act 2003)[48] มาตรา 125 พร้อมทั้งกำหนดคำนิยามที่เกี่ยวข้องไว้ในมาตรา 32 ของพระราชบัญญัติฉบับเดียวกัน ซึ่งมีรายละเอียดของบทบัญญัติและคำนิยามดังต่อไปนี้

มาตรา 125[49] การได้รับบริการการสื่อสารทางอิเล็กทรอนิกส์ อย่างไม่สุจริต

(1) บุคคลใด

(a) โดยไม่สุจริต ได้รับการบริการการสื่อสารทางอิเล็กทรอนิกส์ และ

(b) กระทำโดยมีเจตนาที่จะหลีกเลี่ยงการชำระเงินในค่าใช้จ่ายอันเป็นเงื่อนไขของการได้รับบริการนั้น

เป็นการกระทำที่มีความผิด

มาตรา 32 ความหมายของเครือข่ายและบริการการสื่อสารทางอิเล็กทรอนิกส์

(1) ในพระราชบัญญัตินี้ “เครือข่ายการสื่อสารทางอิเล็กทรอนิกส์[50]” หมายถึง

---

[48] Office of Public Sector Information, “Communications Act 2003,” [Online] Avaliable from : http://www.opsi.gov.uk/acts/acts2003/ukpga_20030021_en_1 (20 ธันวาคม 2551)

[49] 1)A person who—

(a)dishonestly obtains an electronic communications service, and

(b)does so with intent to avoid payment of a charge applicable to the provision of that service,

is guilty of an offence.

[50] 1)In this Act “electronic communications network” means—

(a) ระบบการส่งสัญญาณโดยใช้วิธีการทางไฟฟ้า แม่เหล็ก คลื่นแม่เหล็กไฟฟ้า และ

(b) สิ่งที่ตามมาเหล่านี้ถูกใช้ โดยบุคคลภายใต้เงื่อนไขของระบบและการร่วมมือ เพื่อการส่งสัญญาณ

(i) เครื่องมืออันประกอบในระบบ

(ii) เครื่องมือถูกใช้สำหรับการสับเปลี่ยนหรือการกำหนดเส้นทางของสัญญาณ และ

(iii) ซอฟแวร์หรือข้อมูลที่ถูกเก็บไว้

(2) ในพระราชบัญญัตินี้ “บริการการสื่อสารอิเล็กทรอนิกส์[51]” หมายถึง บริการที่ประกอบด้วยหรือมีลักษณะส่วนใหญ่เป็นการส่งสัญญาณโดยวิธีของเครือข่ายสื่อสารทางอิเล็กทรอนิกส์ของสัญญาณ เว้นแต่เป็นบริการสื่อความหมาย

(a)a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description; and

(b)such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals—

(i)apparatus comprised in the system;

(ii)apparatus used for the switching or routing of the signals; and

(iii)software and stored data.

[51] In this Act “electronic communications service” means a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except in so far as it is a content service.

(10) ในมาตรานี้ “สัญญาณ[52]” รวมถึง

(a) สิ่งต่างๆรวมถึง คำพูด เพลง เสียง ภาพถ่าย หรือ การสื่อสารหรือข้อมูลประเภทใดๆ และ

(b) สัญญาณที่ใช้สำหรับการติดต่อสื่อสารของสิ่งใดๆระหว่างบุคคล ระหว่างบุคคลกับสิ่งใดหรือระหว่างสิ่งใดๆ หรือสำหรับการดำเนินการหรือควบคุมเครื่องมือ

ดังนั้น เมื่อพิจารณาทั้งมาตรา 32 และมาตรา 125 ของพระราชบัญญัติการสื่อสาร ค.ศ. 2003 (Communications Act 2003) ประกอบกัน การกระทำอันเป็นการลักลอบใช้บริการการสื่อสารทางอิเล็กทรอนิกส์ โดยการลักลอบใช้สัญญาณไร้สายของผู้อื่นเพื่อใช้บริการอินเทอร์เน็ตนั้น อาจส่งผลให้ผู้กระทำมีความผิดตามพระราชบัญญัติดังกล่าวได้ซึ่งในประเทศอังกฤษเองก็พบว่ามีการกระทำดังกล่าวเกิดขึ้น[53]

เหตุการณ์นี้เกิดขึ้นที่เขตคริสวิค (Chiswick) ลอนดอนตะวันตก โดยนายเกรกอรี สตราสกีวิคซ (Gregory Straszkiewicz) อายุ 39 ปี ถูกจับกุมเพราะลักลอบใช้บริการอินเทอร์เน็ตบรอดแบนด์ของเพื่อนบ้านที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยไม่ได้รับอนุญาต โดยที่เขาถูกพบว่าอยู่ในบริเวณดังกล่าวหลายครั้งแล้วในรอบ 3 เดือน ทำให้เพื่อนบ้านแจ้งไปยังเจ้าหน้าที่ตำรวจว่าน่าจะมีการกระทำบางอย่างที่น่าสงสัย ซึ่งสุดท้ายแล้วการกระทำของเขาเป็นความผิด

---

[52] In this section “signal” includes—

(a)anything comprising speech, music, sounds, visual images or communications or data of any description; and

(b)signals serving for the impartation of anything between persons, between a person and a thing or between things, or for the actuation or control of apparatus.

[53] “Quardian.co.uk, “Man using laptop on garden wall charged with wireless theft,” [Online] Avaliable from : http://www.guardian.co.uk/uk/2007/aug/23/ukcrime.news และ “Wireless hijacking under scrutiny,” [Online] Avaliable from : http://news.bbc.co.uk/2/hi/technology/4721723.stm) (10 ธันวาคม 2551)

ฐานได้รับบริการโดยไม่ชอบด้วยกฎหมายตามพระราชบัญญัติการสื่อสาร ค.ศ. 2003 (Communications Act 2003) จากการกระทำความผิดนี้ส่งผลให้นายเกรกอรี สตราสกีวิคซถูกปรับเงินจำนวน 500 ปอนด์และถูกคุมประพฤติเป็นเวลา 12 เดือน

4.4.3 ความผิดเกี่ยวกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์เพื่อกระทำความผิด

การกระทำที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์เพื่อกระทำความผิดจะต้องวินิจฉัยตามมาตรา 2 ของ The Computer Misuse Act 1990 ซึ่งได้บัญญัติฐานความผิดที่ซับซ้อนกว่าการกระทำอันเป็นการเข้าถึงระบบโดยปราศจากอำนาจตามมาตรา 1 ที่ไม่ซับซ้อนมากนัก โดยมาตรา 2 มีบทบัญญัติดังต่อไปนี้[54]

---

[54] (1)A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—

(a)to commit an offence to which this section applies; or

(b)to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2)This section applies to offences—

(a)for which the sentence is fixed by law; or

(b)for which a personwho has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous convictions may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the M1Magistrates' Courts Act 1980).

(1) บุคคลที่มีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำผิดตามมาตรา 1 ด้วยเจตนา (มาตรา 1 บัญญัติว่าการไม่มีอำนาจในการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นเป็นความผิด)

(a) ได้กระทำผิดในสิ่งที่มาตรานี้บังคับให้ หรือ

(b) ให้ความสะดวกในการกระทำความผิด (ไม่ว่าโดยตนเองหรือโดยบุคคลใดๆ) และความผิดที่เขาจงใจในการกระทำผิดหรือให้ความสะดวกดังกล่าวต่อไปในมาตรานี้ให้ถือว่าเป็นผู้กระทำผิดเช่นเดียวกับผู้กระทำผิดที่ตนช่วย

(2) มาตรานี้ใช้กับความผิด

(a) ใช้กับความผิดที่ถูกกำหนดไว้ในกฎหมาย

---

(3)It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4)A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5)A person guilty of an offence under this section shall be liable—

(a)on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b)on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c)on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

(b) ใช้กับบุคคลผู้มีอายุ 21 ปีหรือกว่านี้

(3) เพื่อวัตถุประสงค์ของมาตรานี้ไม่ว่าการกระทำความผิดของผู้กระทำผิดที่อยู่ห่างไกล (Remote Hacker) จะได้กระทำลงในโอกาสที่ไม่มีอำนาจในการเข้าถึงระบบนั้นหรือไม่ หรือโดยอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจจะมีความผิดตามมาตรานี้ถึงแม้ว่าจะมีข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำความผิดที่อยู่ห่างไกลจะไม่ได้กระทำลงก็ตาม

(5) บุคคลผู้กระทำผิดตามมาตรานี้ต้องรับผิด

(a) จะพิจารณาคดีแบบรวบรัดและถูกลงโทษจำคุกไม่เกิน 6 เดือนหรือปรับหรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงและถูกลงโทษไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ

เห็นได้ว่าจากบทบัญญัติมาตรา 2 ข้างต้นนี้จะเกี่ยวข้องกับการกระทำอันเป็นการลักลอบเข้าถึงระบบเครือข่ายไร้สายผ่านสัญญาณไร้สายโดยมีเจตนาที่จะกระทำความผิดอื่นๆ หรือให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดการกระทำความผิดร้ายแรงขึ้น อันแตกต่างจากมาตรา 1 โดยมาตรา 1 เป็นกรณีที่ใช้กับการกระทำที่ไม่สามารถพิสูจน์เจตนาในอนาคตได้ ซึ่งจะมีโทษเบากว่า แต่หากพิสูจน์ได้ว่าผู้กระทำมีเจตนาจะกระทำความผิดอย่างอื่น คือ พิสูจน์เจตนาในอนาคตได้ (โดยไม่จำเป็นต้องพิสูจน์ว่าเจตนาในอนาคตนั้นได้มีการกระทำความผิดจริงหรือไม่) จะใช้มาตรา 2 ซึ่งอาจจะเรียกความผิดตามมาตรา 2 ได้ว่า “ความผิดที่ไกลออกไป” ตัวอย่าง[55]ของการกระทำความผิดตามมาตรา 2 นี้ เช่น การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นเพื่อฉ้อโกงตามพระราชบัญญัติฉ้อโกง (The Fraud Act), การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นเพื่อการปลอมแปลงตามพระราชบัญญัติการปลอมแปลง (The Forgery and Counterfeiting Act 1981) เป็นต้น

---

[55] “The Hacking of Computers and the Criminal Law,” [Online] Avaliable from : http://www.inbrief.co.uk/offences/hacking-of-computers.htm) (31 สิงหาคม 2553)

สำหรับในส่วนของผู้ใช้บริการเครือข่ายไร้สายในการใช้งานอินเทอร์เน็ตอาจจะต้องเผชิญกับมาตรการทางกฎหมายหากไม่ดำเนินการตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของตน[56]ตามรายงานของลิเลียน เอดเวิดส์ (Lilian Edwards) ศาสตราจารย์แผนกกฎหมายอินเทอร์เน็ตแห่งมหาวิทยาลัยเชฟฟิลด์ (Sheffield University) ที่ให้รายละเอียดว่า มาตรการทางกฎหมายเช่นนี้มีผลมาจากการที่ศาลเยอรมันได้ตัดสินลงโทษปรับผู้ใช้บริการอินเทอร์เน็ตผ่านสัญญาณไร้สายที่ไม่ได้ตั้งมาตการป้องกันการเข้าถึงเครือข่ายไร้สายของตนไว้ซึ่งเป็นเหตุให้เครือข่ายไร้สายนั้นได้ถูกใช้ในการดาวน์โหลดเพลงโดยผิดกฎหมาย[57]

ลิเลียน เอดเวิดส์ กล่าวต่อไปว่า การตัดสินคดีของศาลเยอรมันเป็นสิ่งที่สะท้อนให้เห็นว่ามันเป็นสิ่งที่ควรจะเกิดขึ้นในประเทศอังกฤษและเป็นการเตือนที่มีคุณค่า แต่อย่างไรก็ตามในขณะนี้กฎหมายยังไม่บังคับในการจำกัดการทำงานของระบบเครือข่าย มันไม่เป็นอาชญากรรมหากเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้แต่มันอาจจะเป็นการผิดเงื่อนไขของผู้ให้บริการอินเทอร์เน็ต

ภายใต้พระราชบัญญัติเศรษฐกิจดิจิทัล (Digital Economy Act) เราอาจได้รับคำเตือนและการยกเลิกการเชื่อมต่ออินเทอร์เน็ตจากผู้ให้บริการถ้าหากเรา “อนุญาต” ให้ใครก็ตามดาวน์โหลดสิ่งผิดกฎหมาย ซึ่งในคณะนี้ยังไม่มีคำนิยามที่แท้จริงของความหมายของคำว่า “อนุญาต” ทำให้การที่เราไม่ได้ตั้งมาตรการป้องกันการเข้าถึงระบบเครือข่ายไว้อาจถือได้ว่าเป็นการ “อนุญาต” ให้ผู้อื่นเข้าใช้งานเครือข่ายไร้สาย

---

[56] “Brits "could face legal action" for leaving Wi-Fi unsecured,” [Online] Avaliable from :

http://www.pcpro.co.uk/news/security/358033/brits-could-face-legal-action-for-leaving-wi-fi-unsecured (12 กรกฎาคม 2553)

[57] “German supreme court fines owner of open WiFi network,” [Online] Avaliable from : http://www.edri.org/edrigram/number8.10/wifi-case-germany-copyright-infringement (30 เมษายน 2554)

บทที่ 5
บทสรุปและข้อเสนอแนะ

อาชญากรรมคอมพิวเตอร์เป็นผลพวงด้านลบที่เกิดขึ้นและขยายตัวมาพร้อม ๆ หรือไล่เลี่ยกับวิวัฒนาการและความก้าวหน้าทางเทคโนโลยีในยุคข้อมูลข่าวสาร ซึ่งในยุคดังกล่าวเกิดนวัตกรรมใหม่อย่างคอมพิวเตอร์และการเชื่อมต่อระหว่างกันจนเกิดเป็นเครือข่ายขนาดเล็ก-ใหญ่ที่เรียกว่าอินเทอร์เน็ต ด้านหนึ่งถูกใช้เป็น "เครื่องมือ" ในการกระทำความผิด ส่วนอีกด้านหนึ่งก็ถูกเล็งให้กลายเป็น "เป้าหมายแห่งการโจมตี" โทษฐานที่เป็นอุปกรณ์ หรือช่องทางสำคัญในการเก็บรักษา และ/หรือ รับ-ส่ง ข้อมูลข่าวสาร ที่ปัจจุบันดูเหมือนจะมีค่ามหาศาลกว่าทรัพย์ประเภทที่มีรูปร่างบางอย่าง เช่น บ้าน รถยนต์ โทรศัพท์เคลื่อนที่ เสียอีก

ปัญหาของอาชญากรรมคอมพิวเตอร์ (Computer Crime) มีความซับซ้อนขึ้นเรื่อย ๆ จนกลายเป็นปัญหาที่แก้ไม่ตกของประเทศทั้งหลาย ทั้งๆที่อาชญากรรมคอมพิวเตอร์เพิ่งเกิดขึ้นและใช้เวลาในการวิวัฒนาการตัวเองในช่วงระยะเวลาเพียงไม่กี่สิบปีเท่านั้น

อย่างไรก็ตาม สิ่งที่น่าวิตกกังวลในการหาทางรับมือกับอาชญากรรมนี้ของประเทศต่าง ๆ ก็คือ จะเห็นได้ว่า ด้วยช่วงระยะเวลาเพียงไม่กี่สิบปี ขอบเขตการทำลายของอาชญากรรมคอมพิวเตอร์ขยายตัวไปสู่ส่วนต่าง ๆ อย่างรวดเร็ว ไม่จำเพาะเจาะจงอยู่ในความเสียหายต่อเศรษฐกิจเท่านั้น โดยมีอินเทอร์เน็ตเป็นตัวเร่งอย่างทรงประสิทธิภาพ

แม้ในปัจจุบัน พัฒนาการในด้านประสิทธิภาพและความสามารถของเทคโนโลยีคอมพิวเตอร์เอง จะเริ่มเกิดภาวะชลอตัวลงไปบ้างแล้ว แต่แนวโน้มที่ภาคส่วนต่าง ๆ ของสังคม จะนำเทคโนโลยีคอมพิวเตอร์ไปใช้เป็นส่วนประกอบ หรือเป็นส่วนหนึ่งของระบบจัดการและเพื่อการพัฒนาศักยภาพการทำงานของตัวเองยังคงมีสูงขึ้นเรื่อย ๆ อย่างต่อเนื่อง ไม่ว่าจะเป็นด้านกองกำลังทหาร, อาวุธสงคราม, การจัดการพลังงาน, ระบบขนส่งทุกประเภท, การศึกษา, ด้านสุขภาพ, ยา, อาหาร โดยเฉพาะอย่างยิ่ง ด้านการค้า ธุรกิจออนไลน์ต่าง ๆ จึงเท่ากับว่าสรรพสิ่งที่กำลังจะตกอยู่ภายใต้การควบคุมโดยคอมพิวเตอร์จะต้องมีการขยายตัวต่อไปเรื่อย ๆ ขอบเขตของอาชญากรรมคอมพิวเตอร์ จึงย่อมสามารถพัฒนา และขยายตัวต่อไปได้อีกไม่จบสิ้น

5.1 บทสรุป

อาชญากรรมคอมพิวเตอร์มีมากมายหลากหลายรูปแบบ การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายก็เป็นอาชญากรรมคอมพิวเตอรูปแบบหนึ่งซึ่งไม่ค่อยมีรายงานการกระทำความผิดเนื่องจากการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของผู้อื่นนั้น ผู้ลักลอบจะดำเนินการเชื่อมต่ออินเทอร์เน็ตโดยอาศัยสัญญาณไร้สาย ซึ่งสัญญาณดังกล่าวเป็นสิ่งที่มองไม่เห็นจึงยากที่เจ้าของเครือข่ายไร้สายซึ่งเป็นผู้มีสิทธิใช้งานอินเทอร์เน็ตจะทราบว่ามีผู้ลักลอบใช้บริการอินเทอร์เน็ตหรือไม่

อย่างไรก็ตาม การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายมีความเกี่ยวข้องเชื่อมโยงกับการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบหรือโดยปราศจากอำนาจเพราะหากผู้ลักลอบต้องการใช้บริการอินเทอร์เน็ตแล้วผู้ลักลอบต้องกระทำการผ่านเข้าถึงระบบคอมพิวเตอร์ของเจ้าของเครือข่ายไร้สายเสียก่อน ดังนั้น หากอ้างอิงตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้ว การลักลอบเข้าถึงระบบคอมพิวเตอร์ที่จะเป็นความผิดก็ต่อเมื่อได้เข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะเท่านั้น โดยไม่ต้องพิจารณาว่าการเข้าถึงนั้นจะเป็นการเข้าถึงโดยมีวัตถุประสงค์ใดหรือไม่

การที่ผู้ใดก็ตามลักลอบเข้าถึงระบบเครือข่ายไร้สายซึ่งถือว่าเป็นการเข้าถึงระบบคอมพิวเตอร์เช่นเดียวกันเพราะระบบเครือข่ายไร้สายเป็นส่วนหนึ่งของระบบคอมพิวเตอร์ตามความหมายของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะส่งผลให้การใช้งานโดยรวมของระบบเครือข่ายไร้สายมีประสิทธิภาพลดลงเนื่องจากมีการส่งข้อมูลในระหว่างเครือข่ายไร้สายเป็นจำนวนมากและอาจเกิดการใช้ระบบคอมพิวเตอร์นั้นในการกระทำความผิดอื่นได้ ดังนั้น หากบัญญัติกฎหมายให้ควบคุมเฉพาะแต่การเข้าถึงระบบคอมพิวเตอร์ที่มีมาตราการป้องกันการเข้าถึงโดยเฉพาะให้เป็นความผิด แต่หากเป็นการเข้าถึงระบบคอมพิวเตอร์ที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ไม่บัญญัติให้เป็นความผิด ย่อมส่งผลให้ผู้ลักลอบสามารถใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของผู้อื่นได้ อีกทั้ง ผู้ลักลอบอาจจะใช้อินเทอร์เน็ตผ่านเครือข่ายไร้สายนั้นในการกระทำความผิดอื่น เช่น การปลอมแปลงลิขสิทธิ์หรือการกระจายภาพอนาจารในระบบอินเทอร์เน็ต เป็นต้น ซึ่งการบัญญัติกฎหมายในลักษณะนี้อาจจะก่อให้เกิดปัญหาในการลงโทษผู้กระทำความผิดเพราะหากผู้ลักลอบได้เข้าไปในระบบเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะ ผู้ลักลอบจะไม่มีความผิดแต่อย่างใด เป็นหน้าที่ของเจ้าของเครือข่ายไร้สายเองที่ต้องตั้งระบบรักษาความปลอดภัยแก่เครือข่ายไร้สายของตน

เมื่อพิจารณาการตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายที่จะต้องดำเนินการทางเทคนิคโดยการเข้าไปตั้งค่ามาตรการป้องกันการป้องกัน (Security) ในอุปกรณ์กระจายสัญญาณไร้สาย หากเจ้าของเครือข่ายไร้สายผู้ใดไม่ได้ตั้งมาตรการป้องกันการเข้าถึงเอาไว้ เครือข่ายไร้สายนั้นจะไม่มีมาตรการป้องกันการเข้าถึงเนื่องจากโรงงานผู้ผลิตอุปกรณ์กระจายสัญญาณไร้สายได้ตั้งค่าให้อุปกรณ์กระจายสัญญาณไร้สายสามารถอนุญาตให้อุปกรณ์ไร้สายทุกเครื่องเข้าสู่ระบบเครือข่ายไร้สายได้โดยไม่ต้องผ่านมาตรการป้องกันการเข้าถึงแต่อย่างใด ดังนั้นในกรณีที่เจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้โดยตนไม่ทราบถึงวิธีการทางเทคนิคในการดำเนินการตั้งค่าและไม่ทราบถึงอันตรายหรือผลเสียหายที่จะเกิดขึ้นจากการไม่ตั้งค่ามาตรการป้องกันการเข้าถึงนั้นจนเป็นเหตุให้มีผู้ลักลอบเข้าสู่เครือข่ายไร้สายเพื่อใช้บริการอินเทอร์เน็ต กฎหมายควรจะให้การคุ้มครองโดยการลงโทษผู้ลักลอบเข้าถึงระบบเครือข่ายไร้สายนั้นหรือไม่

สำหรับกรณีการเข้าถึงระบบเครือข่ายไร้สายของผู้อื่นที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้เพื่ออาศัยอินเทอร์เน็ตของผู้นั้นในการกระทำความผิด การไม่ตั้งมาตรการป้องกันการเข้าถึงดังกล่าวส่งผลให้การลักลอบเข้าถึงระบบเครือข่ายไร้สายเป็นไปได้โดยง่าย จึงมีข้อควรพิจารณาว่าการไม่ตั้งมาตรการป้องกันการเข้าถึงของเจ้าของเครือข่ายไร้สายจนเป็นเหตุให้มีการกระทำความผิดโดยอาศัยเครือข่ายไร้สายนี้ เจ้าของเครือข่ายไร้สายควรจะมีความรับผิดทางอาญาด้วยหรือไม่ เพียงใดเนื่องจากการไม่ระมัดระวังดังกล่าวเป็นการละเลยอันถือได้ว่ามีความประมาทเลินเล่อ

เมื่อพิจารณาแนวทางในการออกกฎหมายที่เกี่ยวข้องกับการเข้าถึงระบบเครือข่ายไร้สายโดยมิชอบในต่างประเทศ เช่น ประเทศสหรัฐอเมริกาและประเทศอังกฤษ ก็ได้มีการกำหนดความผิดที่เกี่ยวข้องกับการเข้าถึงเครือข่ายไร้สายโดยมิชอบเช่นเดียวกันโดยกำหนดเป็นกฎหมายเฉพาะ ดังเช่นในประเทศอังกฤษหรือบัญญัติเพิ่มเติมในประมวลกฎหมายอาญาดังเช่นที่ปรากฏในบางมลรัฐของประเทศสหรัฐอเมริกา ซึ่งผู้เขียนจะได้ยกขึ้นมาพิจารณาเพื่อพิจารณาถึงสิ่งที่คล้ายคลึงกันและสิ่งที่แตกต่างกัน

1. ประเทศสหรัฐอเมริกา

ในประเทศสหรัฐอเมริกา การกำหนดความผิดในการกระทำความผิดที่เกี่ยวข้องกับการเข้าถึงระบบเครือข่ายไร้สายโดยมิชอบจะบัญญัติอยู่ในประมวลกฎหมายอาญาของบางมลรัฐ

แต่จะไม่ได้บัญญัติไว้โดยตรงในกฎหมายของรัฐบาลกลาง ซึ่งในกฎหมายของรัฐบาลกลางในส่วนที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ ที่เรียกว่า The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) ปรากฏอยู่ในมาตรา 1030 อันเป็นบทบัญญัติที่เกี่ยวกับเรื่องฉ้อฉลและกิจกรรมที่เกี่ยวเนื่องกับคอมพิวเตอร์ (18 U.S.C. 1030 Fraud and related activity in connection with computers) มาตรา 2701 เกี่ยวข้องกับการลักลอบเข้าถึงระบบโดยปราศจากอำนาจ แต่ในกรณีนี้เป็นการเข้าถึงข้อมูลการสื่อสารที่ถูกเก็บรักษาไว้ (18 U.S.C. 2701 Unlawful Access to Stored Communications) และมาตรา 1029 อันเป็นบทบัญญัติที่เกี่ยวข้องกับการฉ้อฉลและกิจกรรมที่เกี่ยวเนื่องกับกลไกการเข้าถึง(ระบบเครือข่ายอินเทอร์เน็ต) (18 U.S.C. 1029 Fraud and Related Activity in connection with Access Devices) ซึ่งจากบทบัญญัติทั้งสามมาตราข้างต้นนี้ไม่อาจจะปรับกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายได้เนื่องจากตามบทบัญญัติของกฎหมายมีวัตถุประสงค์หลักเพื่อต้องการคุ้มครองเฉพาะต่อการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบที่กระทบต่อกิจการของรัฐเท่านั้น ไม่รวมถึงการกระทำที่เอกชนกระทำต่อเอกชนตามการวิจัยฉบับนี้

แต่เมื่อพิจารณาตามกฎหมายในบางมลรัฐ พบว่ามีบทบัญญัติที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของผู้อื่นโดยมิชอบ โดยบัญญัติอยู่ใน 2 ลักษณะ

1. การลักลอบใช้บริการอินเทอร์เน็ตของผู้อื่นเป็นความผิดเพราะถือว่าเป็นการกระทำที่เข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจ เช่น กฎหมายของมลรัฐอลาสก้า (Alaska) โดยในบทบัญญัติของกฎหมายบัญญัติแต่เพียงว่าการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นเป็นความผิด ไม่ได้บัญญัติถึงขนาดที่ว่าระบบคอมพิวเตอร์นั้นจะต้องมีมาตรการป้องกันการเข้าถึงโดยเฉพาะด้วย

2. การลักลอบใช้บริการอินเทอร์เน็ตของผู้อื่นเป็นความผิดเพราะถือว่าเป็นการลักลอบใช้บริการ (Theft of Services) เช่น ในกฎหมายของมลรัฐอิลลินอยส์ (Illinois) ที่บัญญัติว่าบุคคลใดกระทำความผิดโดยการลักลอบใช้บริการสัญญาณไร้สาย ถ้ามีเจตนาจะได้รับบริการสัญญาณไร้สายโดยการใช้อุปกรณ์ไร้สายที่ไม่ชอบด้วยกฎหมายหรือปราศจากความยินยอมของผู้ให้บริการสัญญาณไร้สาย ย่อมเป็นความผิดโดยไม่ต้องพิจารณาว่าเครือข่ายไร้สายนั้นได้ตั้งมาตรการป้องกันการเข้าถึงไว้หรือไม่

สำหรับกฎหมายที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์เพื่อกระทำความผิด ไม่ว่าจะเป็นการลักลอบใช้ระบบเครือข่ายไร้สายของผู้อื่นในการส่งภาพอนาจารหรือการลักลอบดาวน์โหลดหรือเผยแพร่สินค้าอันเป็นการละเมิดลิขสิทธิ์

เป็นต้น ได้บัญญัติขึ้นมาเนื่องจากการตระหนักว่าการปล่อยให้เครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้อาจจะเป็นอันตรายต่อระบบข้อมูลที่เก็บรักษาไว้ในระบบคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายไร้สาย ทำให้ในบางเมือง เช่น เมืองเวสท์เชสเตอร์ เคาร์ตี้ มลรัฐนิวยอร์ก (Westchester County, New York) ได้ออกกฎหมายโดยกำหนดให้องค์กรธุรกิจในเมืองจะต้องทำการป้องกันระบบเครือข่ายไร้สายของตน ถ้าระบบเครือข่ายไร้สายนั้นได้ถูกใช้สำหรับการเข้าถึงข้อมูลทางการเงินของลูกค้า ทั้งนี้ทั้งนั้นเพื่อป้องกัน Identity Theft (หรือที่อาจเรียกว่า “การโจรกรรมอัตลักษณ์บุคคล) เช่น หมายเลขบัญชีธนาคาร หมายเลขบัตรประจำตัวประชาชน เพื่อนำไปใช้ในการกระทำความผิด หรือกฎหมายในบางมลรัฐ เช่น กฎหมายของมลรัฐแคลิฟลอเนียร์ (California) ได้กำหนดมาตรการที่เกี่ยวข้องกับการป้องกันการเข้าถึงเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันความปลอดภัย โดยได้กำหนดให้ผู้ผลิต Access Point สำหรับใช้ในสำนักงานขนาดเล็ก, บ้านสำนักงาน (Home Office) หรือบ้านเรือน จะต้องแจ้งเตือนให้ผู้บริโภคทราบถึงวิธีการในการป้องกันการเชื่อมต่อเครือข่ายไร้สายและต้องมีเครื่องหมายเตือนหรือจัดการให้มีการป้องกันอื่นๆ

2. ประเทศอังกฤษ

ในประเทศอังกฤษ การกำหนดความผิดในการกระทำความผิดที่เกี่ยวข้องกับการเข้าถึงระบบเครือข่ายไร้สายโดยมิชอบจะบัญญัติอยู่ในพระราชบัญญัติซึ่งเป็นกฎหมายเฉพาะไม่ได้บัญญัติอยู่ในประมวลกฎหมายอาญาแต่อย่างใด โดยได้บัญญัติอยู่ในกฎหมาย 2 ฉบับดังต่อไปนี้

1. The Computer Misuse Act 1990 จะเป็นกฎหมายที่เกี่ยวข้องกับการเข้าถึงระบบเครือข่ายไร้สายโดยปราศจากอำนาจและการกระทำที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์เพื่อกระทำความผิด แต่อย่างไรก็ตามการเข้าถึงเครือข่ายไร้สายที่จะมีความผิดตามพระราชบัญญัติฉบับนี้จะต้องเป็นการเข้าถึงระบบเครือข่ายไร้สายที่มีมาตรการป้องกันการเข้าถึงด้วย เนื่องจากพระราชบัญญัติฉบับนี้ ในมาตรา 1 ได้บัญญัติว่า “บุคคลจะมีความผิดถ้า

(a) ผู้นั้นได้กระทำการให้คอมพิวเตอร์แสดงผล หรือแสดงการกระทำใดๆโดย**จงใจที่จะผ่านสิ่งป้องกันที่มีไว้เพื่อกันการเข้าถึงระบบ** และได้ทำการผ่านสิ่งป้องกันเช่นว่านั้นเข้าถึง

โปรแกรมคอมพิวเตอร์ใดๆหรือสารสนเทศที่เก็บไว้ในคอมพิวเตอร์หรือทำให้สามารถเข้าถึงคอมพิวเตอร์ที่มีระบบป้องกันอยู่

(b) การผ่านสิ่งป้องกันเข้าไปในระบบหรือทำให้สามารถเข้าถึงคอมพิวเตอร์ที่มีระบบป้องกันนั้น เป็นการกระทำโดยปราศจากอำนาจ และ

(c) บุคคลนั้นได้รู้ขณะที่กระทำอยู่แล้วว่า เขาได้กระทำการอันเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานนั้นปราศจากอำนาจ"

ส่วนตามมาตรา 2 ในพระราชบัญญัติฉบับเดียวกันซึ่งเกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์เพื่อกระทำความผิด ได้บัญญัติว่า "(1) บุคคลที่มีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำผิดตามมาตรา 1 ด้วยเจตนา (มาตรา 1 บัญญัติว่าการไม่มีอำนาจในการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นเป็นความผิด)

(a) ได้กระทำผิดในสิ่งที่มาตรานี้บังคับให้ หรือ

(b) ให้ความสะดวกในการกระทำความผิด (ไม่ว่าโดยตนเองหรือโดยบุคคลใดๆ) และความผิดที่เขาจงใจในการกระทำผิดหรือให้ความสะดวกดังกล่าวต่อไปในมาตรานี้ให้ถือว่าเป็นผู้กระทำผิดเช่นเดียวกับผู้กระทำผิดที่ตนช่วย"

จากบทบัญญัตินี้จึงเห็นได้ว่าการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมีวัตถุประสงค์เพื่อกระทำความผิดที่จะเป็นความผิดนั้นจะต้องเป็นการลักลอบเข้าสู่เครือข่ายไร้สายที่ตั้งมาตรการป้องกันการเข้าถึงเอาไว้ด้วย

2. Communications Act 2003 จะเป็นกฎหมายที่เกี่ยวข้องกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมิชอบ เป็นกฎหมายที่บัญญัติขึ้นเพื่อคุ้มครองเจ้าของเครือข่ายไร้สายผู้มีสิทธิใช้งานอินเทอร์เน็ต โดยจะมีการลงโทษผู้ที่ได้รับบริการการสื่อสารทางอิเล็กทรอนิกส์อย่างไม่สุจริตในลักษณะเป็นความผิดฐานลักลอบใช้บริการ (Theft of Services) ซึ่งการใช้บริการอินเทอร์เน็ตถือเป็นบริการการสื่อสารทางอิเล็กทรอนิกส์ชนิดหนึ่ง ทั้งนี้ไม่ต้องคำนึงว่าเครือข่ายไร้สายนั้นมีมาตรการป้องกันการเข้าถึงหรือไม่

เมื่อได้ทราบถึงกฎหมายต่างประเทศดังกล่าวข้างต้นแล้ว ผู้เขียนจะขอเปรียบเทียบความผิดในส่วนที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบและความผิดฐานลักลอบใช้บริการตามกฎหมายไทยกับกฎหมายของประเทศสหรัฐอเมริกา อังกฤษ ดังต่อไปนี้

1. ทั้งประเทศไทย สหรัฐอเมริกา และอังกฤษต่างกำหนดให้มีความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบซึ่งเป็นความผิดที่สามารถปรับใช้ได้กับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยมิชอบได้ โดยในประเทศไทยและอังกฤษได้บัญญัติฐานความผิดดังกล่าวไว้เป็นพระราชบัญญัติโดยเฉพาะ ขณะที่ประเทศสหรัฐอเมริกาไม่มีบทบัญญัติตามกฎหมายของรัฐบาลกลางที่จะลงโทษกับการกระทำความผิดนี้ได้โดยตรง การลงโทษการกระทำเช่นนี้จึงจะต้องพิจารณาตามประมวลกฎหมายอาญาในแต่ละมลรัฐว่ามีบทบัญญัติในส่วนนี้หรือไม่

2. กฎหมายไทยบัญญัติว่าการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบที่จะเป็นความผิดนั้น จะต้องเป็นการเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะซึ่งมีลักษณะเช่นเดียวกับกฎหมายของประเทศอังกฤษ แต่ในขณะที่กฎหมายอาญาในบางมลรัฐของประเทศสหรัฐอเมริกาไม่ได้บัญญัติองค์ประกอบในส่วนของมาตรการป้องกันการเข้าถึงไว้ ดังนั้น การเข้าถึงเครือข่ายไร้สายโดยมิชอบเพื่อใช้บริการอินเทอร์เน็ต แม้เครือข่ายไร้สายนั้นจะไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้ก็เป็นความผิดแล้ว ดังนั้น หากพิจารณาตามกฎหมายไทย การลักลอบเข้าถึงเครือข่ายไร้สายของผู้อื่นเพื่อใช้บริการอินเทอร์เน็ต หากเครือข่ายไร้สายนั้นไม่มีมาตรการป้องกันการเข้าถึงก็จะไม่เป็นความผิดแต่อย่างใด

3.ประเทศไทยไม่มีบทบัญญัติในลักษณะที่จะลงโทษกับการลักลอบใช้บริการ (Theft of Services) ได้โดยตรงเหมือนดังเช่นกฎหมายอาญาในบางมลรัฐของประเทศสหรัฐอเมริกาหรือประเทศอังกฤษ ทำให้ไม่อาจลงโทษกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายซึ่งถือเป็นการลักลอบใช้บริการชนิดหนึ่งได้ การพิจารณาในการลงโทษกับการกระทำดังกล่าวทำให้ต้องพิจารณาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งเป็นกฎหมายที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบแต่พระราชบัญญัติดังกล่าวไม่ได้บัญญัติลงโทษการลักลอบใช้บริการโดยตรง

เป็นที่น่าสังเกตว่าแม้ในประเทศอังกฤษจะไม่มีรายงานการดำเนินคดีกับการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายโดยอาศัยบทบัญญัติที่กำหนดให้การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบเป็นความผิด ก็อาจจะเป็นเพราะว่าในประเทศอังกฤษมีบทบัญญัติที่ให้ลงโทษกับการลักลอบใช้บริการโดยไม่สุจริตอยู่แล้วนั่นเอง

4. ในประเทศไทยและประเทศอังกฤษยังไม่พบว่ามีกฎหมายที่กำหนดหน้าที่ให้เจ้าของระบบคอมพิวเตอร์จะต้องตั้งมาตรการป้องกันการเข้าถึงระบบของตน แต่ในกฎหมายของ

บางมลรัฐของประเทศสหรัฐอเมริกาได้มีการกำหนดให้เจ้าของเครือข่ายไร้สายหรือเจ้าของอุปกรณ์กระจายสัญญาณไร้สายต้องตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของตนหรือผู้ผลิตอุปกรณ์กระจายสัญญาณไร้สายจะต้องแจ้งเตือนแก่เจ้าของเครือข่ายไร้สายถึงอันตรายที่อาจจะเกิดขึ้นกับเครือข่ายไร้สายของตนและมาตรการป้องกันอันตรายนั้นๆ ทั้งนี้ก็เพื่อเป็นการให้ความระมัดระวังหรือลดอาชญากรรมที่อาจจะเกิดขึ้นจากการกระทำความผิดอื่นที่อาศัยอินเทอร์เน็ตโดยผ่านเครือข่ายไร้สาย

5.2 ข้อเสนอแนะ

เมื่อผู้เขียนได้ศึกษาเนื้อหาตามวิทยานิพนธ์ฉบับนี้อย่างละเอียดแล้ว ผู้เขียนมีข้อเสนอแนะดังต่อไปนี้

1. การบัญญัติกฎหมาย

การระงับยับยั้งการกระทำอันเป็นอาชญากรรมคอมพิวเตอร์ วิธีการที่ดีที่สุดและได้รับการยอมรับอย่างเป็นสากล ก็คือการบัญญัติกฎหมายเพื่อลงโทษกับการกระทำความผิดที่เกิดขึ้นหรืออาจจะเกิดขึ้นได้ต่อไปในภายหน้า การลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการลักลอบใช้เครือข่ายไร้สายของผู้อื่นในการกระทำความผิดเป็นความผิดที่ยังพบได้ไม่บ่อยในสังคมไทยทำให้อาจจะมีปัญหาในการบังคับใช้กฎหมายอยู่บ้าง ดังนั้น จึงสมควรที่จะต้องมีการแก้ไขหรือเพิ่มเติมบทบัญญัติของกฎหมายที่มีผลบังคับอยู่ในปัจจุบัน ดังต่อไปนี้

1.1 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 การที่บัญญัติให้การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบเป็นความผิดเฉพาะการเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงเท่านั้น เป็นเรื่องที่สมควรแล้วเพราะการตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สาย แม้เป็นวิธีการทางเทคนิคแต่ผู้ที่ใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายในฐานะเป็นผู้รับบริการย่อมจะต้องมีความรู้ความเข้าใจในลักษณะการทำงานของระบบอินเทอร์เน็ต ไม่ว่าจะเป็นวิธีการเชื่อมต่อหรือระบบการรักษาความปลอดภัยก็ตาม ทั้งนี้เนื่องจากภัยอันตรายที่เกี่ยวข้องกับอินเทอร์เน็ตเป็นสิ่งที่ทุกคนสามารถรับรู้ได้อยู่แล้วว่ามีอยู่จริงและอาจสร้างผลกระทบที่ร้ายแรงต่อตนเองได้ การไม่ตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายก็ย่อมถือได้ว่าเจ้าของเครือข่ายไร้สายไม่ได้หวงกันในการที่ผู้อื่นจะเข้ามาใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายของตน ประเด็นที่สมควรจะพิจารณาปรับเปลี่ยนแก้ไขก็มีอยู่แต่เพียงความหมายของคำว่า “โดยมิชอบ” ว่าควรจะมีความหมายกว้างหรือแคบเพียงใด โดยอาจจะบัญญัติให้ความหมายไว้ในส่วนของคำนิยาม

1.2 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่มีบทบัญญัติที่เอาผิดการลักลอบใช้บริการเหมือนกับที่ปรากฏในกฎหมายของบางมลรัฐในประเทศสหรัฐอเมริกาหรือประเทศอังกฤษ ดังนั้น หากรัฐเห็นว่าการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายสมควรจะเป็นความผิดตามกฎหมายอาญาเพราะเป็นการลักลอบใช้บริการอินเทอร์เน็ตที่เจ้าของเครือข่ายไร้สายไม่ได้แสดงเจตนาอย่างชัดแจ้งในการให้เข้าใช้บริการ ก็อาจจะบัญญัติไว้เป็นฐานความผิดฐานลักลอบใช้บริการการสื่อสารทางอิเล็กทรอนิกส์โดยไม่สุจริตก็ได้

1.3 การที่เจ้าของเครือข่ายไร้สายไม่ได้ตั้งมาตรการป้องกันการเข้าถึงไว้อาจจะเป็นเหตุให้มีผู้ลักลอบเข้าใช้เครือข่ายไร้สายนั้นในการกระทำความผิดได้โดยง่ายเนื่องจากไม่ต้องผ่านมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์แต่อย่างใด อีกทั้งการสืบย้อนหลังเพื่อทราบถึงผู้กระทำความผิดที่แท้จริงทำได้ยากเพราะผู้ลักลอบเมื่อได้เชื่อมต่อเข้าสู่เครือข่ายไร้สายและกระทำความผิดแล้วก็อาจจะไม่ได้อยู่ในบริเวณนั้นอีกต่อไป และการกระทำดังกล่าวก็ยากที่จะมีประจักษ์พยานที่เห็นการกระทำความผิดนั้น ดังนั้น จึงควรที่จะมีบัญญัติของกฎหมายในลักษณะลงโทษเจ้าของเครือข่ายไร้สายที่ไม่ได้ตั้งมาตรการป้องกันการเข้าถึงของตนจนเป็นเหตุให้มีผู้ลักลอบใช้เครือข่ายไร้สายนั้นในการกระทำความผิด

1.4 ในการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์นั้น ควรที่จะกำหนดบทเพิ่มโทษในกรณีที่เป็นการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบโดยมีวัตถุประสงค์ในการกระทำความผิดอื่น เช่น ลักลอบเข้าใช้บริการอินเทอร์เน็ตผ่านสัญญาณไร้สายในการประกาศภาพลามกอนาจารหรือเผยแพร่สินค้าละเมิดลิขสิทธิ์ เนื่องจากการกระทำดังกล่าวมีความร้ายแรงและความเสียหายมากกว่าการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบทั่วๆไป

1.5 ควรกำหนดบทบัญญัติของกฎหมายที่กำหนดให้ผู้ให้บริการอินเทอร์เน็ต (ISP) หรือผู้ผลิตอุปกรณ์กระจายสัญญาณไร้สายซึ่งเป็นเครื่องมือที่อำนวยให้เกิดการใช้งานเครือข่ายไร้สายมีหน้าที่แจ้งเตือนให้แก่ผู้รับบริการอินเทอร์เน็ตหรือผู้บริโภคที่ซื้ออุปกรณ์กระจายสัญญาณไร้สายไปถึงมาตรการในการป้องกันการเข้าถึงเครือข่ายไร้สาย เนื่องจากผู้รับบริการหรือผู้บริโภคบางรายไม่ทราบถึงวิธีการตั้งมาตรการป้องกันการเข้าถึงเครือข่ายไร้สายของตนซึ่งการตั้งมาตรการป้องกันดังกล่าวล้วนเป็นวิธีการทางเทคนิค

2. การใช้มาตรการอย่างอื่น

ในบางครั้งการใช้มาตรการทางกฎหมายในการบังคับกับการกระทำความผิดที่เกิดขึ้นเพียงอย่างเดียวอาจไม่สามารถลดปัญหาการประกอบอาชญากรรมลงได้อย่างมีประสิทธิภาพเท่ากับการนำมาตรการในส่วนอื่นๆมาเสริมกับมาตรการทางกฎหมาย ซึ่งมาตรการอย่างอื่นที่สมควรมาเสริมกับมาตรการทางกฎหมายในการลดปัญหาการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการลักลอบใช้เครือข่ายไร้สายของผู้อื่นในการกระทำความผิด มีดังต่อไปนี้

2.1 เผยแพร่ความรู้เรื่องอาชญากรรมคอมพิวเตอร์โดยเฉพาะอย่างยิ่งกรณีการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายแก่ผู้ใช้คอมพิวเตอร์ หน่วยงาน องค์กรต่างๆ ให้เข้าใจแนวคิดวิธีการของอาชญากรทางคอมพิวเตอร์เพื่อป้องกันตนจากการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายและการกระทำความผิดอื่นโดยอาศัยเครือข่ายไร้สาย เช่น การรณรงค์ให้เจ้าของเครือข่ายไร้สายดำเนินการตั้งค่ามาตรการป้องกันการเข้าถึงระบบเครือข่ายไร้สายหรือจัดตั้งหน่วยงานให้บริการหรือให้คำแนะนำในการตั้งค่ามาตรการป้องกันการเข้าถึงดังกล่าว

2.2 ส่งเสริมจริยธรรมในการใช้คอมพิวเตอร์ ทั้งโดยการสร้างความรู้ความเข้าใจแก่บุคคลทั่วไปในการใช้คอมพิวเตอร์อย่างถูกต้อง และโดยการปลูกฝังเด็กตั้งแต่ในวัยเรียนให้เข้าใจกฎเกณฑ์ มารยาทในเรื่องการใช้คอมพิวเตอร์และเครือข่ายดังกล่าว

สรุป ภัยอันตรายที่เกิดขึ้นกับอาชญากรรมคอมพิวเตอร์ไม่ว่าจะเป็นการลักลอบใช้บริการอินเทอร์เน็ตผ่านเครือข่ายไร้สายหรือการลักลอบใช้เครือข่ายไร้สายของผู้อื่นในการกระทำความผิด เป็นภัยอันตรายที่นับวันยิ่งเกิดขึ้นบ่อยโดยเฉพาะอย่างยิ่งในต่างประเทศ แม้ว่าปัจจุบันในประเทศไทย ปัญหาดังกล่าวยังไม่พบบ่อยนักแต่การเฝ้าดูเพื่อยับยั้งมิให้เกิดปัญหาหรือกำหนดมาตรการในการรับมือหากเกิดปัญหาขึ้นในอนาคตก็นับว่าเป็นสิ่งที่ดีเพราะเป็นที่แน่นอนว่าการป้องกันไม่ให้ปัญหาเกิดย่อมดีกว่าการปล่อยให้เกิดปัญหาและตามแก้ไข ซึ่งการขจัดปัญหาอาชญากรรมคอมพิวเตอร์ดังกล่าวนี้ต้องอาศัยทั้งมาตรการทางกฎหมายและมาตรการทางด้านอื่นๆควบคู่กันไป แต่สิ่งที่สำคัญที่สุดก็คือในการแก้ไขปัญหาใดๆก็ตามนั้นจะต้องอาศัยความร่วมมือของทุกๆองค์กรในประเทศ ไม่ว่าจะเป็นหน่วยงานราชการ ธุรกิจของเอกชน หรือแม้กระทั่งปัจเจกชนก็ตาม ทั้งนี้ ก็เพื่อให้สังคมได้ดำเนินไปอย่างราบรื่นปราศจากภัยอันตรายนั่นเอง

รายการอ้างอิง

ภาษาไทย

จักกริช พฤษการ. การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Communication and Networking. กรุงเทพมหานคร : ท้อป, 2549.

ชาตรี ส่งสัมพันธ์. อาชญากรรมคอมพิวเตอร์ : ศึกษาวิเคราะห์การเข้าถึงโดยมิชอบ. วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2552.

ญาณพล ยั่งยืน. " อาชญากรรมทางคอมพิวเตอร์. [ออนไลน์] แหล่งที่มา : http://elib.coj.go.th/Article/49_9_8.pdf [2554, เมษายน 30]

ณัฐวุฒิ ทรัพย์บุญมี. CDMA คืออะไร. [ออนไลน์] แหล่งที่มา : http://pirun.kps.ku.ac.th/~b4928057/1.html [2553, ตุลาคม 12]

เดอะลอร์ดออฟไวร์เลสดอทคอม (thelordofwireless.com). [ออนไลน์] แหล่งที่มา : http://www.thelordofwireless.com [2554, มกราคม 10]

ทวีเกียรติ มีนะกนิษฐ. คำอธิบายกฎหมายอาญาภาคทั่วไป. กรุงเทพมหานคร : วิญญูชน, 2551.

ธวัชชัย ชมศิริ. ติดตั้ง/ดูแล ระบบเครือข่ายคอมพิวเตอร์อย่างมืออาชีพ. กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น, 2549.

ฟอร์ด แอนตี้ ทรัสต์ส บลอค (Ford AntiTrust's Blog). ระบบเครือข่ายไร้สาย (Wireless LAN). [ออนไลน์] แหล่งที่มา : http://www.thaicyberpoint.com/ford/blog/id/194 [2552, กันยายน 11]

พรเพชร วิชิตชลชัย. คำอธิบาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. กรุงเทพมหานคร : สำนักงานศาลยุติธรรม, 2550.

พิญดา เลิศกิตติกุล. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์. วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550.

ฤทธิไกร ขัณฑวีระมงคล.ผู้ก่อตั้งเว็บไซต์ http://www.adslthailand.com. สัมภาษณ์, 25 ธันวาคม 2553.

เลิศชาย สุธรรมพร. อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล. วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขาวิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2541.

โลกกว้างแห่งเทคโนโลยีสารสนเทศ. [ออนไลน์] แหล่งที่มา : http://www.widebase.net/knowledge/itterm/it_term_desc.php?term_id=hub [2553, สิงหาคม 11]

วิกิพีเดีย สารานุกรมเสรี. แบนด์วิดท์. [ออนไลน์] แหล่งที่มา : http://th.wikipedia.org/wiki/%E0%B9%81%E0%B8%9A%E0%B8%99%E0%B8%94%E0%B9%8C%E0%B8%A7%E0%B8%B4%E0%B8%94%E0%B8%97%E0%B9%8C [2553, กันยายน 13]

วิกิพีเดีย สารานุกรมเสรี. เอดจ์ (เครือข่ายไร้สาย). [ออนไลน์] แหล่งที่มา : http://th.wikipedia.org/wiki/%E0%B9%80%E0%B8%AD%E0%B8%94%E0%B8%88%E0%B9%8C_%28%E0%B9%80%E0%B8%84%E0%B8%A3%E0%B8%B7%E0%B8%AD%E0%B8%82%E0%B9%88%E0%B8%B2%E0%B8%A2%E0%B9%84%E0%B8%A3%E0%B9%89%E0%B8%AA%E0%B8%B2%E0%B8%A2%29 [2553, ตุลาคม 12]

วิรินทร์ เมฆประดิษฐสิน. รอบรู้ระบบการทำงานของ NAT ตอนเชื่อมต่ออินเทอร์เนตอย่างปลอดภัยและประหยัด. [ออนไลน์] แหล่งที่มา : http://www.paktho.ac.th/computerptk/introcom/nat.htm [2553, ธันวาคม 14]

วีระพงษ์ บุญโญภาส. อาชญากรรมทางเศรษฐกิจ. กรุงเทพมหานคร : สำนักพิมพ์นิติธรรม, 2552.

ศัพท์น่ารู้เกี่ยวกับ CDMA. [ออนไลน์] แหล่งที่มา : http://www.bloggang.com/viewblog.php?id=mr-kong&date=24-10-2006&group=1&gblog=2 [2553, ธันวาคม 14]

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์. [ออนไลน์] แหล่งที่มา : http://www.etcommission.go.th/books/Cyber_crime.pdf [2552, กันยายน 14]

สถาบันนวัตกรรมและพัฒนากระบวนการเรียนรู้. คอมพิวเตอร์น่ารู้. [ออนไลน์] แหล่งที่มา : http://www3.ipst.ac.th/research/assets/web/mahidol/computer%2810%29/network/net_wan9.htm [2552, กันยายน 10]

สมเกียรติ รุ่งเรืองลดา. Internet Sharing สำหรับระบบ LAN ในองค์กรและ Internet Cafe. ฉบับพิมพ์ครั้งที่ 1. กรุงเทพมหานคร : โปรวิชั่น, 2544.

สุธี พงศาสกุลชัยและณรงค์ ล่ำดี. การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์. ฉบับพิมพ์ครั้งที่ 1. กรุงเทพมหานคร : เคทีพี คอมพ์ แอนด์ คอนซัลท์, 2551.

สำนักคอมพิวเตอร์ มหาวิทยาลัยมหิดล. เทคโนโลยี Multicast. [ออนไลน์] แหล่งที่มา : http://www.cc.mahidol.ac.th/newsletter/Old/Vol7/content_1.htm [2552, กันยายน 11]

สำนักงานคณะกรรมการกฤษฎีกา (กฎกระทรวงออกตามความในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550). [ออนไลน์] แหล่งที่มา : http://www.krisdika.go.th [2553, สิงหาคม 11]

สำนักงานเลขาธิการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์. ฉบับพิมพ์ครั้งที่ 2. กรุงเทพมหานคร :

สำนักงานฯ, 2547.

อาณัติ รัตนถิรกุล. รายนามศูนย์บริการอินเทอร์เน็ต (ISP) ในไทย.[ออนไลน์] แหล่งที่มา : http://www.arnut.com/isp.php [2553, สิงหาคม 3]

องอาจ เทียนหิรัญ. อาชญากรรมทางคอมพิวเตอร์ : การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์. วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2546.

อนันต์ ผลเพิ่ม. แลนไร้สาย (Wireless LAN). กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น, 2550.

อรรณพ ขันธิกุลและอำนาจ มีมงคล. ติดตั้งและใช้งาน Hi Speed Internet. ฉบับพิมพ์ครั้งที่ 1. นนทบุรี : ไอดีซีฯ, 2549.

อรรณพ ขันธิกุลและอำนาจ มีมงคล. ออกแบบและติดตั้งระบบ Wireless LAN. ฉบับพิมพ์ครั้งที่ 1. นนทบุรี : ไอดีซีฯ, 2547.

อรรณพ ขันธิกุลและอำนาจ มีมงคล. ออกแบบและติดตั้งระบบ Wireless LAN 2nd edition. ฉบับพิมพ์ครั้งที่ 1. นนทบุรี : ไอดีซีฯ, 2553.

เอดีเอสแอลไทยแลนด์ (adslthailand). กฎหมายอาชญากรรมคอมพิวเตอร์. [ออนไลน์] แหล่งที่มา : http://www.adslthailand.com/forum/viewtopic.php?t=681 [2552, สิงหาคม 5]

แอกเน่เทค (ACNETECH). Modulation. [ออนไลน์] แหล่งที่มา : http://www.acentech.net/cms/index.php?option=com_content&task=view&id=428&Itemid=205 [2553, ธันวาคม 10]

ภาษาอังกฤษ

AB 2415. [Online] Available from :

http://www.leginfo.ca.gov/pub/05-06/bill/asm/ab_2401-2450/ab_2415_bill_20060930_chaptered.html [2010, April 12]

Alaska Legal Resource Center. [Online] Available from :

http://touchngo.com/lglcntr/akstats/STATUTES/Title11/Chapter46/Section740.htm [2008, December 10]

Arstechnica. WiFi freeloader arrested in Washington. [Online] Available from :

http://arstechnica.com/old/content/2006/06/7111.ars) [2008, December 10]

Bangeman,E. RIAA loses in file sharing case. [Online] Available from :

http://arstechnica.com/old/content/2006/07/7257.ars [2010, October 25]

Bangeman,E. The Ethics of "Stealing" a WiFi Connection. [Online] Available from :

http://arstechnica.com/security/news/2008/01/the-ethics-of-stealing-a-wifi-connection.ars [2010, October 25]

Brits could face legal action for leaving Wi-Fi unsecured. [Online] Available from :

http://www.pcpro.co.uk/news/security/358033/brits-could-face-legal-action-for-leaving-wi-fi-unsecured [2010, July 12]

Capitol v. Thomas.[Online] Available from :

http://en.wikipedia.org/wiki/Capitol_v._Thomas [2010, May 1]

CBSNEWS. Man Arrested For Stealing Wi-Fi. [Online] Available from :

http://www.cbsnews.com/stories/2005/07/07/tech/main707361.shtml [2009, August 10]

Clough,J. Principles of Cybercrime. [Online] Available from :

http://books.google.co.th/books?id=JVPnCqEuTksC&pg=PR17&lpg=PR17&dq=Ellis+v+DPP+2001&source=bl&ots=GLQbPIbXII&sig=2Et8vue1XTwb2r1mBScc

cb29hZM&hl=th&ei=B6UuTfDBI8KxrAeSz4S6Cg&sa=X&oi=book_result&ct=result&resnum=9&ved=0CFAQ6AEwCA#v=onepage&q=Ellis%20v%20DPP%202001&f=false [2010, June 30]

Computer Crime & Intellectual Property Section. United States Department of Justice. [Online] Available from : http://www.justice.gov/criminal/cybercrime/ccmanual/03ccma.html [2009, March 19]

Computer Misuse Act 1990. [Online] Available from : http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences [2009, March 13]

Computer Misuse Act Explained. [Online] Available from : http://knol.google.com/k/norman-creaney/computer-misuse-act-explained/1hzaxtdr9c09g/8#) [2010, August 14]

Cybertelecom Federal Internet Law & Policy An Educational Project. WiFi Theft / Piggy Backing :: Security. [Online] Available from : http://www.cybertelecom.org/broadband/wifisecurity.htm [2010, January 15]

Fisher,K. The RIAA, IP addresses, and evidence. [Online] Available from : http://arstechnica.com/old/content/2006/08/7416.ars) [2010, October 25]

Foxnews. MICHIGAN MAN FINED FOR USING COFFEE SHOP'S WI-FI NETWORK. [Online] Available from : http://www.foxnews.com/story/0,2933,276720,00.html) [2009, March 6]

German court orders wireless passwords for all Users can be fined if a third party takes advantage of an open connection. [Online] Available from : http://www.msnbc.msn.com/id/37107291/ns/technology_and_science-security [2011, January 12]

German supreme court fines owner of open WiFi network. [Online] Avaliable from : http://www.edri.org/edrigram/number8.10/wifi-case-germany-copyright-infringement [2011, April 30]

House of Lord : Judgments -- Director of Public Prosecutions v. McKeown Director of Public Prosecutions v. Jones. [Online] Available from : http://www.publications.parliament.uk/pa/ld199697/ldjudgmt/jd970220/mcke01.htm [2010, June 16]

Judge, S.S. and Amanda, M.H. Background paper harmonizing national and legal approaches on cyber. [Online] Available from : http://www.itu.int/osg/spuold/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf [2011, Febraury 11]

Illinois WiFi freeloader fined US$250. [Online] Avaliable from : http://arstechnica.com/old/content/2006/03/6447.ars [2009, January 2]

Illinois General Assembly. CRIMINAL OFFENSES (720 ILCS 5/) Criminal Code of 1961. [Online] Available from : http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=072000050HArt.+16F&ActID=1876&ChapterID=53&SeqStart=36700000&SeqEnd=37400000 [2008, December 20]

Law in the Last Mile : Sharing Internet Access Through WiFi. [Online] Available from : http://www.law.ed.ac.uk/ahrc/script-ed/vol6-2/macsithigh.asp [2010, September 12]

Law of New York. [Online] Available from : http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYD

ATA=$$PEN156.00$$@TXPEN0156.00+&LIST=LAW+&BROWSER=BROWSER+&TOKEN=37356239+&TARGET=VIEW [2010, November 11]

New5. Movie Company Files Federal Piracy Suit Against Tri-State Man. [Online] Available from : http://www.wlwt.com/health/5520020/detail.html [2010, December 25]

New law requires some businesses to secure their WiFi networks. [Online] Available from : http://arstechnica.com/old/content/2006/04/6647.ars [2011, January 10]

N.J. Student Secretly Taped Having Sex in Dorm Posted Suicide Plunge Message on Facebook. [Online] Available from : http://www.foxnews.com/us/2010/09/29/rutgers-students-accused-secretly-taping-sex-dorm-posting-video-online [2011, January 10]

Office of Public Sector Information. Communications Act 2003. [Online] Available from : http://www.opsi.gov.uk/acts/acts2003/ukpga_20030021_en_1 [2008, December 20]

Office of Public Sector Information. Computer Misuse Act 1990. [Online] Available from: http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm [2008, December 20]

Office of Public Sector Information. The Police and Justice Act 2006. [Online] Available from : http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060048_en.pdf) [2008, December 20]

Palmer police seize computer of man using free wireless. [Online] Available from : http://torgo-x.livejournal.com/tag/libraries [2008, December 10]

Quardian.co.uk. Man using laptop on garden wall charged with wireless theft. [Online] Available from : http://www.guardian.co.uk/uk/2007/aug/23/ukcrime.news [2008, December 10]

RIAA Discontinued Case in California, Virgin v. Marson. [Online] Available from : http://recordingindustryvspeople.blogspot.com/2006/07/riaa-discontinued-case-in-california.html [2010, October 23]

RIAA Drops Open WiFi Case – Virgin v. Marson. [Online] Available from : http://daledietrich.com/imedia/riaa-drops-open-wifi-case-virgin-v-marson [2010, October 23]

RIAA Rips Defendant in Nation's First Filesharing Jury Trial. Online] Available from : http://www.wired.com/threatlevel/2007/10/riaa-rips-defen [2010, May 1]

Sophos Press Release. Wi-Fi piggybacking widespread, Sophos research reveals. [Online] Available from : http://www.sophos.com/pressoffice/news/articles/2007/11/wi-fi.html [2010, September 3]

6 Reasons Why You Should Secure Your Unsecured Wi-Fi Wireless Network, What Can Happen, What To Do (such as porn). [Online] Available from : http://hubpages.com/hub/6-Reasons-Why-You-Should-Secure-Your-Wi-Fi-Network [2010, July 31]

Stockwel,l J. WiFi Turns Internet Into Hideout for Criminals. [Online] Available from : http://www.washingtonpost.com/wp-dyn/content/article/2007/02/10/AR2007021001457.html [2010, May 1]

Suicide of Megan Meier. [Online] Available from : http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier [2011, January 10]

The Free Dictionary By Farlex. [Online] Available from : http://legal-dictionary.thefreedictionary.com/Gross+negligence [2010, June 24]

The Hacking of Computers and the Criminal Law. [Online] Available from : http://www.inbrief.co.uk/offences/hacking-of-computers.htm) [2010, August 31]

Two cautioned over wi-fi 'theft. [Online] Available from : http://news.bbc.co.uk/2/hi/uk_news/england/hereford/worcs/6565079.stm [2010, Febraury 26]

UNITED STATES CODE § 1029. Fraud and related activity in connection with computers. [Online] Available from : http://www.law.cornell.edu/uscode/18/usc_sec_18_00001029----000-.html [2008, December 8]

UNITED STATES CODE § 1030. Fraud and related activity in connection with computers. [Online] Available from : http://www.justice.gov/criminal/cybercrime/1030NEW.htm [2008, December 10]

UNITED STATES CODE § 2701. Unlawful access to stored communications. [Online] Available from : http://www.law.cornell.edu/uscode/18/usc_sec_18_00002701----000-.html [2008, December 8]

Unsecured internet connection leads to law enforcement raid. [Online] Available from : http://www.winknews.com/Local-Florida/2010-10-07/Unsecure-internet-connection-leads-to-law-enforcement-raid [2010, February 2]

Unsecured wireless owners being sued by victims. [Online] Available from : http://www.dba-oracle.com/oracle_news/2005_7_29_wireless_owners_sued.htm [2009, September 10]

Westchester's Wi-Fi Legislation. [Online] Available from : http://consumer.westchestergov.com/index.php?option=com_content&view=article&id=2600&Itemid=100081 [2011, January 2]

Wikipedia. the free encyclopedia. Computer Fraud and Abuse Act. [Online] Available from : http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act [2008, December 6]

Wikipedia. the free encyclopedia. Computer Misuse Act 1990. [Online] Available from : http://en.wikipedia.org/wiki/Computer_Misuse_Act_1990 [2008, December 20]

Wireless hijacking under scrutiny. [Online] Available from : http://news.bbc.co.uk/2/hi/technology/4721723.stm [2008, December 10]

ภาคผนวก

หน้า ๔
เล่ม ๑๒๔ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

เป็นปีที่ ๖๒ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

หน้า ๕
เล่ม ๑๒๔ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ

จะต้องรับโทษภายในราชอาณาจักร

หมวด ๒
พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

หน้า ๕
เล่ม ๑๒๔ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้วพนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หน้า ๑๐
เล่ม ๑๒๔ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา ๒๐ ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา ๒๑ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

ประวัติผู้เขียนวิทยานิพนธ์

นายบุญทัศน์ ยังน้อย เกิดเมื่อวันที่ 14 สิงหาคม 2526 จังหวัดกรุงเทพมหานคร จบการศึกษาระดับอุดมศึกษาจากคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีการศึกษา 2548 สอบไล่ได้ความรู้ชั้นเนติบัณฑิต สมัยที่ 60 ปีการศึกษา 2550 เข้าศึกษาต่อในระดับปริญญาโท ปีการศึกษา 2550 ปัจจุบันประกอบอาชีพทนายความอิสระ