แนวทางปฏิบัติตามกฎหมายการเก็บข้อมูล ฯ สำหรับผู้ดูแลและพัฒนาเว็บ

พัฒนพงศ์ สุนทรกำจรพานิช
สมาคมผู้ดูแลเว็บไทย
info@webmaster.or.th

ที่มา

ก่อนหน้าจะมีกฎหมายเกี่ยวกับความผิดทางคอมพิวเตอร์ ทางผู้ดูแลและพัฒนาระบบเว็บไซด์ต่างขาดซึ่งแนวทางการปฏิบัติที่ชัดเจนในการเก็บข้อมูล ตามที่กฎหมายกำหนด จนกระทั่งกลางปี 50 **พระราชบัญญัติ ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550** ได้ประกาศใช้เมื่อวันที่ 21 สิงหาคม 2550 แม้ว่าจะมีกฎหมายออกมาชัดเจน ตามที่กำหนดในตัวบทกฎหมายแล้ว แต่ก็ยังไม่มีแนวทางปฏิบัติที่เป็นรูปธรรมโดยเฉพาะอย่างยิ่ง ในส่วนที่เกี่ยวข้องกับเว็บไซด์ ซึ่ง ผู้ประกอบการ, เจ้าของ, นักพัฒนาระบบ ควรที่จะได้รับรู้แนวทางปฏิบัติที่ถูกต้องเพื่อที่จะได้เตรียมการให้พร้อมก่อน **ระยะเวลาผ่อนผัน 1 ปี** ตามที่กฎหมายกำหนด จะสิ้นสุดลงในวันที่ 20 สิงหาคม 2551 (ระยะเวลาผ่อนผันจะกล่าวถึงเฉพาะ กรณี ผู้ให้บริการเว็บ ตามข้อ 10 ประกาศกระทรวง ฯ เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ 2550 นอกเหนือจากข้อ 10 (1) และ ข้อ 10 (2)) หากว่าผู้ให้บริการเว็บไซด์ไม่ปฏิบัติตามกฎหมาย จะมีระวางโทษปรับสูงถึง **500,000** บาท ตามมาตรา 26 วรรคสาม ใน พรบ ฯ ซึ่งทางสมาคมผู้ดูแลเว็บไทย เห็นความจำเป็นเร่งด่วนในส่วนนี้ที่จะส่งเสริมให้ความรู้ความเข้าใจและแนะนำแนวทางปฏิบัติที่เป็นรูปธรรม เพื่อให้ผู้ประกอบการด้านเว็บนำไปประยุกษ์ใช้ให้เหมาะสมกับระบบของแต่ละท่านที่ใช้อยู่ เพื่อไม่ให้เกิดปัญหาทำผิดกฎหมายโดยรู้เท่าไม่ถึงการขึ้นในภายหลัง และเนื่องจากกฎหมายฉบับบนี้พูดถึงความผิดในหลาย ๆ ด้าน แต่ในกรณีนี้จะกล่าวเจาะลึกไปถึงเฉพาะสิ่งที่ผู้ดูแลและพัฒนาเว็บจะต้องทำตามกฎหมายเป็นเบื้องต้นก่อน

กฎหมายที่เกี่ยวข้องโดยตรง

- พระราชบัญญัติ ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550
- ประกาศกระทรวงเทคโน ฯ เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ 2550
- ประกาศกระทรวงเทคโน ฯ เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ ตาม พรบ ฯ ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550

แนวปฏิบัติตามกฎหมาย

จากเนื้อหาที่เขียนไว้ใน **พระราชบัญญัติ ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550** พอสรุปเป็นแนวทางสำหรับนักพัฒนา เป็นเงื่อนไขดังนี้คือ

การให้บริการบนเว็บทุกประเภทที่เป็นการให้บริการนั้น ย่อมเข้าข่ายตามกฎหมายนี้เพราะทั้งหมดเป็น **Content and Application Service Provider** ถ้าเราทำเว็บไม่ว่าเพื่อตนเองหรือบุคคลอื่น ย่อมเข้าข่ายนี้ทั้งสิ้น หมายความว่าคนที่เป็นเจ้าของเว็บย่อมเป็น "ผู้ให้บริการ" ตามความหมายใน ข้อ 5 (2) และต้องมีหน้าที่ดังต่อไปนี้

1. **เก็บข้อมูลผู้ใช้บริการ และ บันทึกเข้าใช้ข้อมูล**
2. **เก็บข้อมูลของผู้ประกาศ ในกรณีที่เป็น Web board หรือ Blog**
3. **เวลาใน log ที่เก็บจะต้องตั้งให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยให้ผิดพลาดไม่เกิน ๑๐ มิลลิวินาที**
4. **ที่เก็บข้อมูล (ตัว log) จะต้อง กำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าวเพื่อรั กษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้**
5. **เก็บข้อมูล (ตัว log) ไว้เป็นเวลา 90 วัน นับตั้งแต่เกิดกิจกรรมนั้น จะเก็บยาวกว่านั้น ตามที่ เจ้าพนักงานสั่ง แต่ไม่เกิน 1 ปี**

1 เก็บข้อมูลผู้ใช้บริการ และ บันทึกเข้าใช้ข้อมูล

ตามวัตถุประสงค์ของกฎหมายมุ่งที่จะมองหาตัวผู้กระทำการ ในกรณีมีผู้กระทำผิดกฎหมาย ในขณะที่มองในมุมมองของนักพัฒนาและเจ้าของเว็บเราไม่มีทางรู้ได้โดยแท้ว่าใครเป็นใครบนระบบ สิ่งที่เรารู้มีเพียง **"ข้อมูลด้านเทคนิค"** และ **"ข้อมูลจาก Information"** ผู้ให้บริการไม่จำเป็นต้องรับผิดชอบว่า ข้อมูลด้านเทคนิค หรือ ด้าน Information นั้น จะเป็นของบุคคลใดในการพิสูจน์ในศาลหรือไม่ เพียงแต่ว่าจะต้องเก็บข้อมูลให้เป็นข้อมูลที่ถูกต้องเมื่อเข้ามาสู่ระบบของผู้ให้บริการเท่านั้นเป็นพอ เช่น

IP Address

ไม่ต้องสนใจว่าเป็น IP Proxy หรือ IP จริง ส่วนของประเภทของ IP ของที่ระบบมองเห็นนั้นจะเป็น IP จริงหรือไม่นั้น เราไม่ต้องไปสนใจ สิ่งที่จะต้องสนใจคือขอให้การเก็บข้อมูล IP ที่ระบบมองเห็นนั้นให้ทำโดยอัตโนมัติและควรจะต้องเก็บ IP 2 ชุด เพื่อความถูกต้องซึ่งก็ได้แก่ **Private IP** (IP ภายใน) กับ **Public IP** (IP จริง) ซึ่งสำหรับระบบของผู้พัฒนานั้นจะปรากฏ Private IP หรือไม่ปรากฏ ก็ไม่เป็นไร ขอให้ขั้นตอนในการเก็บมีครบถ้วนตามนั้น เป็นพอ ตัวอย่างเช่น

192.168.1.13:203.155.8.108

ระบบหากว่ามองไม่เห็น IP ภายใน อาจจะเห็นแค่

: 203.155.81.158

เป็นต้น ตัวอย่าง การเขียนบนภาษา PHP เพื่อเก็บ IP ในเอกสารประกอบด้านล่าง

ข้อมูลจาก Information

จากตัวประกาศ เขียนไว้ว่า "ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ หรือ เลขประจำตัว (User ID) ของผู้ขายสินค้าหรือบริการ หรือ เลขประจำตัวผู้ใช้บริการ (User ID) และที่อยู่บนจดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ" ซึ่งจริง ๆ แล้วหมายถึงข้อมูลที่ปรากฏ ของผู้ใช้บริการที่ ส่งเข้ามาโดยวิธีต่าง ๆ เช่น กรณีเป็นระบบสมาชิก ผู้พัฒนา จะต้องเก็บ ข้อมูลการสมัคร อยู่แล้ว ซึ่งก็ไม่ต้องสนใจว่าข้อมูลนั้น จะจริงแท้หรือไม่ ขอให้บันทึกโดยอัตโนมัติ แล้วบุคคลอื่นไม่สามารถเข้าแก้ไขในส่วนของบุคคลนั้น ๆ ได้เป็นการเพียงพอ ตัวอย่างที่เราต้องเก็บก็ได้แก่

- User ID
- ข้อมูลที่ User นั้นกรอกเข้ามา (ตัวอย่างเช่น ชื่อ นามสกุล ที่อยู่ Email ฯลฯ)
- เวลาสมัคร

บันทึกเข้าใช้ข้อมูล

บันทึกเข้าใช้ข้อมูลนะที่นี่ ผมขอแนะนำให้เก็บเป็น 2 กรณี เนื่องจากหากว่าเราเก็บทุก ๆ กิจกรรมที่ User นั้น ๆ ทำ จะเกิด log ของ user จำนวนมหาศาล ซึ่งถ้าผู้ให้บริการเว็บ รายไหนอยากจะเก็บก็สามารถทำได้ ครับ แต่ที่แนะนำและสามารถทำได้โดยไม่ลำบากเกินไปนั้น คือแนะนำให้เก็บตามนี้คือ

1 กรณี Login เข้าสู่ระบบ

กรณีนี้ในความถูกต้องแท้จริงของข้อมูลนั้น (ได้แก่ **IP Address, เวลา**) บอกเราได้แค่ว่า User คนนั้นเข้าสู่ระบบเมื่อไหร่บ้าง เหตุที่ไม่ได้เน้นการ Log off เพราะ การ logoff บนระบบ web นั้น ไม่แน่นอน ข้อมูลการ login ในกรณีนี้จึงเก็บในฐานเหมือนพยานแวดล้อมที่บอกว่า User นั้น ๆ เข้าสู่ระบบเมื่อใดบ้าง

2 กรณี เกิดกิจกรรม Get หรือ Post ข้อมูลที่จะปรากฏ เข้าสู่ระบบ

กรณีข้อมูลที่เก็บ (ได้แก่ **IP Address, เวลา**) ตามกรณีตรงนี้คือหัวใจสำคัญของการเก็บ log ให้ถูกต้องตามกฎหมาย การเก็บ ณ ขณะนี้ ย่อมพิสูจน์ ความแท้จริง ณ ขณะมีคนกระทำความผิดจริง ๆ เป็นพยานหลักฐานโดยตรง ที่จะพิสูจน์และระบุตัวผู้กระทำผิด ทำไมเป็นเช่นนั้นเพราะ ถ้าลองวิเคราะห์ ความผิดที่ปรากฏบน internet ในกรณีต่าง ๆ ก็เกิดจากการ **Get และ Post ให้ข้อมูลมาปรากฏทั้งสิ้น** เช่น กรณีหมิ่นประมาท, หลอกลวง, ฉ้อโกง, ขุ่กรรโชก, ขายของผิดกฎหมาย ฯลฯ (กล่าวถึงเฉพาะความผิดที่จะเกี่ยวข้องกับเว็บในแง่ผู้ใช้บริการและผู้ให้บริการ) สิ่งที่พิสูจน์ ณ ขณะนี้ระบบบอกแค่เพียงว่า **"IP Address นี้กระทำการตามที่ปรากฏในเว็บ ณ ขณะเวลาที่บันทึกไว้"** ซึ่งก็เป็นหน้าที่ของกระบวนการยุติธรรมที่จะดำเนินการค้นหาตัวผู้กระทำความผิดต่อไป ไม่เกี่ยวข้องกับเราเพียงแค่เราต้องให้ข้อมูลที่เก็บอย่างถูกต้องและชัดเจนเป็นเพียงพอ

2 เก็บข้อมูลของผู้ประกาศ ในกรณีที่เป็น Web board หรือ Blog

ในแง่ทางปฏิบัติ กรณีเป็น Web board หรือ Blog มักจะเกิดปัญหาอยู่สม่ำเสมอกรณีมีการแจ้งว่ามีข้อความที่ปรากฏปัญหา เช่น หมิ่นประมาท, ข้อความฉ้อโกง ผู้พัฒนาระบบมักชอบทำระบบลบข้อความโดนการลบทิ้งไปเลย ซึ่งจริง ๆ โดยแท้ไม่ควรรีบลบทิ้ง เพราะเป็นการทำลายหลักฐานในกรณี ที่ผู้เสียหายมีความ

จำเป็นต้องใช้ข้อมูลนั้น ในศาล อาจจะมีการร้องขอข้อมูลมายังผู้ดูแลได้ในอนาคต ผู้พัฒนาระบบเว็บ ควรออกแบบระบบในรูปแบบที่เป็นการแสดงข้อมูลตาม **Status** ให้ระบบแสดงผล เฉพาะ สถานะที่กำหนด เท่านั้น เพื่อที่จะยังรักษาข้อมูลไว้นำส่ง เจ้าพนักงานเจ้าหน้าที่ เมื่อมีการร้องขอ ตัวอย่าง วิธีการเก็บข้อมูลที่ดี

ID	UserID	Title	Detail	Time	IP	Status
1	29	หัวข้อ	ข้อมูลปรกติ	2008-04-08 11:11:59	192.168.1.13:203.155.8.108	TRUE
2	51	หัวข้อ	ข้อมูลที่มีปัญหาทางกฎหมาย	2008-04-08 11:11:59	:58.10.8.100	False

สถานะ **False** คือจะไม่แสดงข้อมูลนี้จากทุก ๆ ส่วนของระบบ ในกรณีที่เกรงว่าข้อมูลจะล้นจากระบบ เราสามารถ ย้าย ข้อมูลในสถานะ **false** ไปยัง Table backup ได้ในอนาคต หรือลบบางส่วนทิ้งเมื่อพ้นระยะเวลาเก็บตามกฎหมาย

หรืออีกวิธีหนึ่งคือเลือกเก็บข้อมูล Backup ในรูปแบบของ **Text file** หรือ รวมเป็น folder ไปในกรณีที่มีข้อมูลอื่น ๆ ประกอบเช่น (file ภาพ, file Video, file download) เก็บยัง **folder** ที่อยู่นอก path ของ web server ที่คนทั่วไปไม่สามารถเข้าถึงได้ ตัวอย่าง เช่น

ข้อมูลที่เป็นปัญหาอยู่ที่
http://www.content.com/board/1049.html
path เดิมอยู่ที่ web server คือ /**data_web**/board/1049.html
ควรย้ายไป นอก web server /**del_data_web**/board/1049.html

3 เวลาใน log ที่เก็บจะต้องตั้งให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยให้ผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

กรณีนี้อยากให้ผู้พัฒนา , เจ้าของเว็บ และ ผู้ดูแลระบบให้ความใส่ใจในส่วนนี้ให้มากเนื่องจากในทางปฏิบัติเกิดปัญหามากมายเรื่องการตั้งเวลาบน Server คลาดเคลื่อนเป็นอย่างมาก จนกลายเป็นเรื่องเดือดร้อนยังผู้ที่ไม่ได้เกี่ยวข้องเพราะระบบโดยส่วนใหญ่ของ User ผู้ใช้ Internet ในประเทศเป็นแบบ Dynamic IP เมื่อ เชื่อมต่อ Internet หนึ่งครั้งจะได้ IP ที่ ISP จะสุ่มขึ้นมาแจกให้ User นั้น ๆ 1 ชุด เมื่อ Internet เกิดหลุด หรือ หยุดการเชื่อมต่อ แล้วมีการต่อใหม่ก็จะได้ IP ใหม่ อีก 1 ชุด ในขณะที่ IP ชุดเดิมก็จะนำไปวนใช้ใหม่เมื่อ User คนอื่นเข้าเชื่อมต่อ Internet ยก ตัวอย่างเช่น

มี User A เชื่อมต่อ Internet แล้วไปเขียนบนเว็บบอร์ดขู่ฆ่า ประธานาธิบดี ประเทศ B จากนั้นก็ Disconnect การเชื่อมต่อไป หลังจากนั้นบังเอิญว่า User C Connect เชื่อมต่อ Internet จากผู้ให้บริการรายเดียวกันพอดี ระบบ สุ่มให้ IP Address ที่ User A เคยใช้ไปให้ User C แต่ระบบ Server ที่เก็บข้อมูลดันตั้งเวลาคลาดเคลื่อนไป 1 นาที จากข้อมูล log ทำให้เข้าใจว่า User C เป็นคนทำ

อันนี้เป็นตัวอย่างปัญหาที่มีความเป็นไปได้ในการเกิดเหตุ เฉพาะฉะนั้นผู้ดูแลระบบ Server ควรตั้งเวลาให้ถูกต้องจริง ๆ ผมขอแนะนำให้ติดตั้ง **Network Time Protocol** (NTP) บน server เพื่อ ให้อ้างอิงเวลากับ

server ที่ได้รับการยอมรับ อย่างเช่น Server ของ Nectec อ่าน วิธีการติดตั้ง NTP Server ง่าย ๆ ใน เอกสารประกอบทางเทคนิคด้านล่าง

4 ที่เก็บข้อมูล (ตัว log) จะต้อง กำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าวเพื่อรั กษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้

ในกรณีนี้กฎหมายเขียนเป็นแนวทางไว้โดยวัตถุประสงค์คือ ต้องเก็บข้อมูลไว้ไม่ให้เข้าถึงโดยใครก็ได้ (หมายถึงข้อมูล Log) โดยในกฎหมายแนะนำให้ใช้วิธีการ อย่างเช่น Centralized Log Server หรือการ ทำ Data Archiving หรื อทำ Data Hashing ซึ่งในกรณีองค์กรใหญ่ ๆ จะมีปัญหาน้อยเพราะใช้วิธีซื้อ ระบบเก็บ Log เอาเลย ปัญหาคือใน level เล็ก ๆ หรือเป็นบุคคลธรรมดา ควรให้ความสนใจในจุดนี้ โดย เนื้อแท้แล้ว คือ **" ทำให้ข้อมูล Log ไม่สามารถเข้าถึงได้ และแก้ไขไม่ได้"** สำหรับระบบ web หากว่า ออกแบบระบบให้ตอบโจทย์นี้ได้ก็ย่อมได้รับการยอมรับ ในความถูกต้องของข้อมูลยกตัวอย่าง เช่น

- ตั้ง User และ Database แยกต่างหาก ไม่รวมกับ User ใช้งาน หรือ user ที่ใช้งานนั้น เข้าถึงได้แค่ Insert แต่ไม่สามารถ Update หรือ delete ได้ เป็นต้น
- เก็บ log file ไว้ใน folder ที่เข้าถึงได้เฉพาะ admin

5 เก็บข้อมูล (ตัว log) ไว้เป็นเวลา 90 วัน นับตั้งแต่เกิดกิจกรรมนั้น จะเก็บยาวกว่านั้น ตามที่ เจ้าพนักงานสั่ง แต่ไม่เกิน 1 ปี

เรื่องนี้ตรงตัวเลยครับ ไม่มีอะไรคือหมายถึง "log" เก็บไว้ ตามมาตราฐานคือ 90 วัน ในกรณีที่เจ้า พนักงาน ตาม พรบ มีคำสั่งให้เก็บนานกว่านั้นแต่ไม่เกิน 1 ปี

โดยสรุปการเก็บข้อมูลจราจรทางคอมพิวเตอร์นั้นมีวัตถุประสงค์เพื่อที่จะรับษาความถูกต้อง และใช้เป็น หลักฐานตามกฎหมายในการยืนยันการกระทำผิด เป็นคนละกรณีกับการพูดเรื่องเสรีภาพไม่ว่าจะทางความคิด หรืออื่น ๆ ซึ่งจริง ๆ แล้วคนที่จะเข้าถึง log ได้กฎหมายก็กำหนดตัวบุคคลที่จะเข้าถึงได้อย่างชัดเจน และการ เปิดเผยข้อมูลใด ๆ จะทำโดยพละการไม่ได้ รวมทั้งมีความผิดตามกฎหมายหากเปิดเผย ในขณะที่โลกจริง ยังมีคน ทำผิดกฎหมาย การกลั่นแกล้ง ต่าง ๆ นา ๆ ในฐานะที่เราต่างก็เป็นผู้ให้บริการระบบที่มักจะทำหน้าที่เป็นสื่อ แบบ เปิด เราความมีความรับผิดชอบต่อสังคม เป็นส่วนร่วมในการปกป้องผู้เสียหาย ด้วย ในขณะเดียวกันก็เพื่อป้องกัน ตนเองจากการกระทำผิดโดยไม่รู้ตัว ทางผมและสมาคมผู้ดูแลเว็บไทย หวังว่าเอกสารเผยแพร่นี้จะเป็นแนวทาง ในทางปฏิบัติที่จะช่วยแก้ปัญหาให้ทุกท่านได้

หลักกฎหมายที่เกี่ยวข้องโดยตรงที่ผู้ดูแลและพัฒนาเว็บควรรู้

ในส่วนนี้ผมได้ตัดรวบรวมส่วนที่เกี่ยวข้องและมีความสำคัญหลัก ๆ ของ พรบ ฉบับนี้ โดยจะมองกฎหมายเฉพาะในแง่ การจัดเก็บข้อมูลเท่านั้น เพราะถ้าว่าโดยภาพรวมทั้งหมดในความผิดที่อาจจะเกิดนั้นมีมหาศาล และจะกว้างเกินความจำเป็นที่นักพัฒนาและเจ้าของเว็บไซต์จำเป็นต้องรู้ ในบทความนี้จะพูดถึงเฉพาะกรณีเป็นหน้าที่ หลัก ๆ ที่จะต้องทำโดยเคร่งครัดเท่านั้น ในส่วนหลักกฎหมายตามเนื้อความด้านล่างนี้ มีร่วมด้วยเพื่อไว้เป็นหลักกฎหมายในการอ้างอิง โดยผมจะอธิบายขั้นตอนและวิธีการ ไว้ในด้านหลังโดนละเอียดอีกที อยากให้อ่านตัวกฎหมายแบบ ให้ผ่านตาไปซักรอบก่อน จะทำความเข้าใจได้โดยง่ายขึ้น

- **พระราชบัญญัติ ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550**

  มาตรา 3 ในพระราชบัญญัตินี้

  .....

  "ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

  .....

  "ผู้ให้บริการ" หมายความว่า

  .....

  (2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

  "ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

  มาตรา 26 **<u>ผู้ให้บริการ</u>**ต้องเก็บรักษา**<u>ข้อมูลจราจรทางคอมพิวเตอร์</u>**ไว้ไม่น้อยกว่า**<u>เก้าสิบวัน</u>** นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น**พนักงานเจ้าหน้าที่**จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

  ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

  ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

  ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ **<u>ต้องระวางโทษปรับไม่เกินห้าแสนบาท</u>**

- **ประกาศกระทรวงเทคโน ฯ เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ 2550**

ข้อ 5 ภายใต้บังคับของมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แบ่งได้ ดังนี้

.....

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่นตาม (1) (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่าง ๆ (Application Service Provider) ประกอบด้วยผู้ให้บริการดัง **ภาคผนวก ก.** แนบท้ายประกาศนี้

.....

ข้อ 7 ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ดังนี้

.....

(5) ผู้ให้บริการตาม ข้อ 5 (2) มีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. 4

ทั้งนี้ ในการเก็บรักษาข้อมูลจราจรตามภาคผนวกต่าง ๆ ที่กล่าวไปข้างต้นนั้น ให้ผู้ให้บริการเก็บเพียงเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น

ข้อ 8 การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(1) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(2) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าวเพื่อรั กษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรื อทำ Data Hashing เป็นต้น เว้นแต่ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กร กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรื อบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

(๓) จัดให้มีผู้มีหน้าที่ประสานงาน และให้ข้อมูลกับพนักงานเจ้าหน้าที่ ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้การส่งมอบ ข้อมูลนั้นเป็นไปด้วยความรวดเร็ว

(๔) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

(๕) ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ ๑ ถึงข้อ ๔ ข้างต้น ได้ ให้บริการในนามตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุ ให้ ผู้ให้บริการในข้อ ๑ ถึงข้อ ๔ ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการ เช่นว่านั้นต้องดำเนินการให้มี วิธีการระบุและยืนยันตัวบุ คคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

ข้อ 9 เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริง ผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

.....

ผู้ให้บริการอื่นนอกจากที่กล่าวมาในข้อ 10 (1) และข้อ 10 (2) ข้างต้น ให้เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งปีนับจากวันประกาศในราชกิจจานุเบกษา

ภาคผนวก ก

แนบท้ายประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

.....

.....

2. ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตามข้อ 5 (2) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก แนบท้ายประกาศนี้

ประเภท	ตัวอย่างของผู้ให้บริการ
ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่าง ๆ (Content and Application Service Provider)	1) ผู้ให้บริการเว็บบอร์ด (Web board) หรือ ผู้ให้บริการบล็อค (Blog) 2) ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเตอร์เน็ต (Internet Banking) และผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Electronic Payment Service Provider) 3) ผู้ให้บริการเว็บเซอร์วิส (Web Service) 4) ผู้ให้บริการพาณิชย์อิเล็คทรอนิกส์ (e-Commerce)หรือ ธุรกรรมทางอิเล็กทรอนิกส์ (e-Transactions)

ภาคผนวก ข

แนบท้ายประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

.....

.....

4.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศ ข้อ 5 (2) มีหน้าที่ต้องเก็บรักษามีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)	1). ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ หรือ เลขประจำตัว (User ID) ของผู้ขายสินค้าหรือบริการ หรือ เลขประจำตัวผู้ใช้บริการ (User ID) และที่อยู่บนจดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ

	2). บันทึกข้อมูลเข้าใช้บริการ **3). กรณีผู้ให้บริการเว็บบอร์ต (Web board) หรือ ผู้ให้บริการบล็อค (Blog) ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล**

<u>ตัวอย่าง code ภาษาต่าง ๆ ในการเก็บ IP Address ทั้ง Private IP และ Public IP</u>

PHP

```
/// ตัวอย่าง function เก็บ IP

function getip()
{
 $cad="";
 if(isset($_SERVER['HTTP_X_FORWARDED_FOR']) AND
    $_SERVER['HTTP_X_FORWARDED_FOR']!="")
            $cad=$_SERVER['HTTP_X_FORWARDED_FOR'];
 if(isset($_SERVER['REMOTE_ADDR']) AND
   $_SERVER['REMOTE_ADDR']!="")
            $cad=$_SERVER['REMOTE_ADDR].":".$cad;
  return $cad;
}

$ip = getip();

/// output  192.168.1.13:203.155.8.108
```

JSP

```
<%
try {
   // get ip of customer
   String strPrivateIP = request.getHeader("x-forwarded-for");

   if(strPrivateIP == null || strPrivateIP.compareTo("") == 0) {
      strPrivateIP = request.getHeader("HTTP_X_FORWARDED_FOR");
   }

   out.println("Private IP : " + strPrivateIP + "<br>");

   out.println("Public IP : " + request.getRemoteAddr());

   //java.net.InetAddress i = java.net.InetAddress.getLocalHost();
   //out.println("Private IP  : " + i.getHostAddress() + "<br>");

}catch(Exception e){
    e.printStackTrace();
}
%>
```

ASP

```
    Function GetIP()
```

```
    GetIP = Request.ServerVariables("HTTP_X_FORWARDED_FOR")
    If GetIP="" Then GetIP = Request.ServerVariables("REMOTE_ADDR")
End Function
```

Python

```
PUBLICIP = cgi.os.environ['REMOTE_ADDR']
PRIVATEIP = cgi.os.environ['HTTP_X_FORWARDED_FOR']
```

Ruby on Rails

```
@client_ip = request.remote_ip
```