มูลนิธิศูนย์สารสนเทศเครือข่ายไทย
นายชยา ลิมจิตติ
ดร.ยรรยง เต็งอำนวย
นางเพ็ญศรี อรุณวัฒนามงคล
ดร.พจนันท์ รัตนไชยพันธ์

ข้อมูลส่วนบุคคลในระบบชื่อโดเมน

ปรับปรุง 5 มิถุนายน 2563

ระบบชื่อโดเมนคืออะไร

ก่อนจะทำความเข้าใจระบบชื่อโดเมนต้องเริ่มด้วยการอธิบายเกี่ยวกับระบบอินเทอร์เน็ตโดยย่อเสียก่อน อินเทอร์เน็ตคือเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อกันโดยใช้โปรโตรคอล TCP/IP อุปกรณ์ใด ๆ ที่จะรับส่งข้อมูลในระบบอินเทอร์เน็ตจะต้องมีหมายเลข โดยหมายเลขในเครือข่ายอินเทอร์เน็ตมีชื่อทางเทคนิคว่าหมายเลขไอพี อย่างไรก็ตามมนุษย์ซึ่งเป็นผู้ใช้งานอินเทอร์เน็ตนั้นไม่คุ้นเคยกับการจดจำหมายเลข ตัวอย่างเช่นระบบโทรศัพท์จะอ้างอิงเครื่องโทรศัพท์ด้วยหมายเลข แต่ผู้ใช้งานจะคุ้นเคยกับชื่อบุคคลหรือสถานที่ มากกว่า ดังนั้นจึงมีสมุดโทรศัพท์ (ที่เป็นกระดาษและไม่ใช่กระดาษ) ที่ช่วยให้ผู้ใช้งานบันทึกชื่อกับหมายเลขโทรศัพท์ไว้ด้วยกัน ในระบบอินเทอร์เน็ตก็เช่นกัน ผู้ใช้งานอ้างอิงการติดต่อในโลกอินเทอร์เน็ต ด้วยชื่อเช่น ชื่ออีเมลหรือชื่อเว็บแต่อุปกรณ์ต่าง ๆรับส่งข้อมูลโดยใช้ หมายเลขไอพี ระบบที่อยู่เบื้องหลังและทำหน้าที่แปลงชื่อไปเป็นหมายเลขไอพีคือระบบชื่อโดเมน (Domain Name System: DNS)

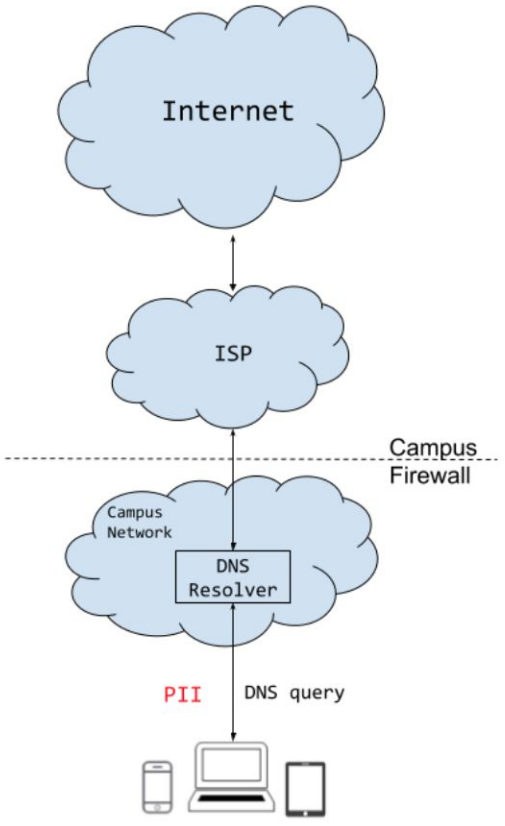
ระบบชื่อโดเมนเป็นส่วนประกอบที่สำคัญมากของระบบอินเทอร์เน็ต ทุกครั้งที่มีการใช้งานระบบใด ๆ บนอินเทอร์เน็ตเช่น พร้อมเพย์ LINE Facebook หรืออ่านเมล ระบบชื่อโดเมนจะเป็นขั้นตอนแรกที่ถูกเรียกใช้งาน หากระบบชื่อโดเมนไม่สามารถทำงานได้ ผู้ใช้งานจะไม่สามารถใช้งานระบบใด ๆ บนอินเทอร์เน็ตได้เลย นอกจากนี้ระบบค้นหาข้อมูลรายใหญ่ของโลก เช่น Google ก็ต้องอาศัยระบบชื่อโดเมนเช่นกันเพราะการเริ่มเก็บข้อมูล จากเว็บต่าง ๆ ทั่วโลกนั้นต้องเริ่มจากการแปลงชื่อเว็บเหล่านั้นไปเป็น หมายเลขไอพีเสียก่อน หากระบบชื่อโดเมนไม่สามารถทำงานได้ Google ก็ไม่สามารถเก็บข้อมูลได้ ดังนั้นจึงสามารถสรุปได้ว่าระบบชื่อโดเมนเป็น โครงสร้างพื้นฐานที่สำคัญมากของระบบอินเทอร์เน็ต

ระบบชื่อโดเมนกับข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personally Identifiable Information: PII) หมายถึงข้อมูลที่สามารถระบุถึงตัวบุคคลได้ทั้งทางตรงและทางอ้อม ทั้งนี้หมายเลขไอพีเป็นข้อมูลส่วนบุคคลทางอ้อมประเภทหนึ่ง เพราะเมื่อนำข้อมูลนี้ไปประกอบกับข้อมูลอื่น ๆ ก็จะสามารถระบุตัวบุคคลที่ใช้งานหมายเลขไอพีนั้น ๆ ได้ และพิจารณาการทำงานของอุปกรณ์ใด ๆ ขณะใช้งานอินเทอร์เน็ตแล้วจะพบว่าทุกครั้งที่ผู้ใช้ใช้งานอินเทอร์เน็ต อุปกรณ์ของผู้ใช้จะสอบถามข้อมูลชื่อโดเมน (DNS Query) ไปที่ DNS Resolver ก่อนเสมอ ดังนั้น DNS Resolver จึงทราบ (และอาจจัดเก็บ) หมายเลขไอพีของผู้ใช้ได้ และนอกจากทราบหมายเลขไอพีแล้ว DNS Resolver ยังรู้อีกด้วยว่าผู้ใช้ดังกล่าวกำลังทำกิจกรรมใดบนอินเทอร์เน็ตโดยดูจากชื่อโดเมนที่อุปกรณ์นั้น ๆ สอบถามมายัง DNS Resolver ดังนั้นข้อมูลชื่อโดเมนจึงเป็นข้อมูลส่วนบุคคลประเภทหนึ่ง

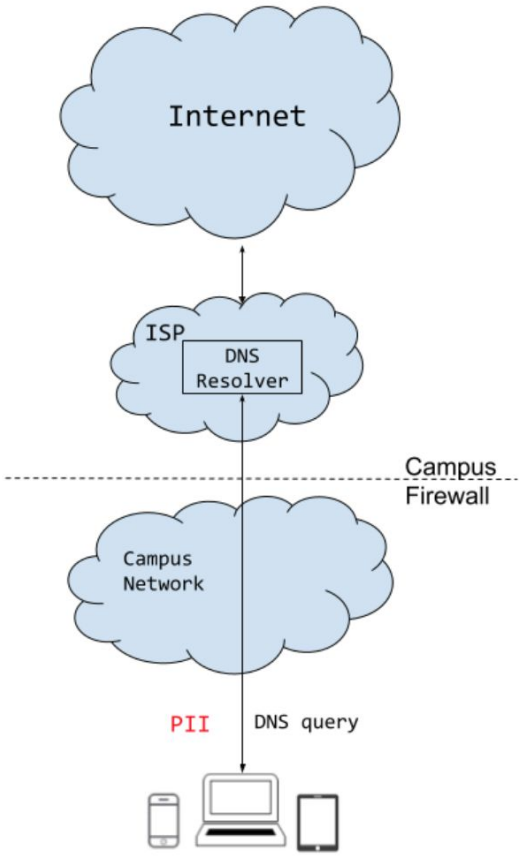
โครงสร้างอินเทอร์เน็ตและระบบชื่อโดเมนกับประเด็นเรื่องการละเมิดข้อมูลส่วนบุคคล

ในยุคแรกของอินเทอร์เน็ตนั้น การเชื่อมต่ออินเทอร์เน็ตจำกัดอยู่เฉพาะหน่วยงานด้านการศึกษา การวิจัย หน่วยงานของรัฐ และหน่วยงานเอกชนบางหน่วยงานเท่านั้น การเชื่อมต่ออินเทอร์เน็ตและการติดตั้ง DNS Resolver เป็นไปตามรูปที่ 1 กล่าวคือทุกหน่วยงานจะมี DNS Resolver เป็นของตัวเอง ดังนั้นการควบคุมข้อมูลส่วนบุคคลที่อาจถูกบันทึกไว้ ณ DNS Resolver นั้นจะเป็นไปภายใต้การควบคุมและนโยบายของหน่วยงานนั้น ๆ ทั้งนี้การได้มาซึ่งข้อมูลส่วนบุคคลในกรณีนี้เป็นไปตามเหตุเพื่อการปฏิบัติตามสัญญา (Contract Basis) เพราะมีความจำเป็นที่ DNS Resolver จะต้องได้ข้อมูลหมายเลขไอพีของผู้ใช้ มิฉะนั้นผู้ใช้จะไม่สามารถใช้งานอินเทอร์เน็ตได้



รูปที่ 1 แสดงที่ตั้ง DNS Resolver ณ เครือข่ายคอมพิวเตอร์ภายในหน่วยงาน

ต่อมาเมื่อการใช้งานอินเทอร์เน็ตขยายตัวไปสู่หน่วยงานต่าง ๆ มากขึ้น หน่วยงานบางแห่งอาจจะไม่มี DNS Resolver ของตัวเอง แต่จะใช้บริการ DNS Resolver จาก ISP ที่เชื่อมต่อด้วย แม้หน่วยงานจะไม่ได้ดูแล DNS Resolver เอง แต่เนื่องจากหน่วยงานมีสัญญากับ ISP ที่เชื่อมต่อด้วย ดังนั้นหน่วยงานก็ยังสามารถกำกับดูแลข้อมูลส่วนบุคคลที่เกิดขึ้น ณ DNS Resolver ได้ผ่านทางสัญญาที่ทำกับ ISP อนึ่งการได้มาซึ่งข้อมูลส่วนบุคคลในกรณีนี้เป็นเพื่อการปฏิบัติตามสัญญา (Contract Basis) เพราะมีความจำเป็นที่ DNS Resolver จะต้องได้ข้อมูลหมายเลขไอพีของผู้ใช้ มิฉะนั้นผู้ใช้จะไม่สามารถใช้งานอินเทอร์เน็ตได้



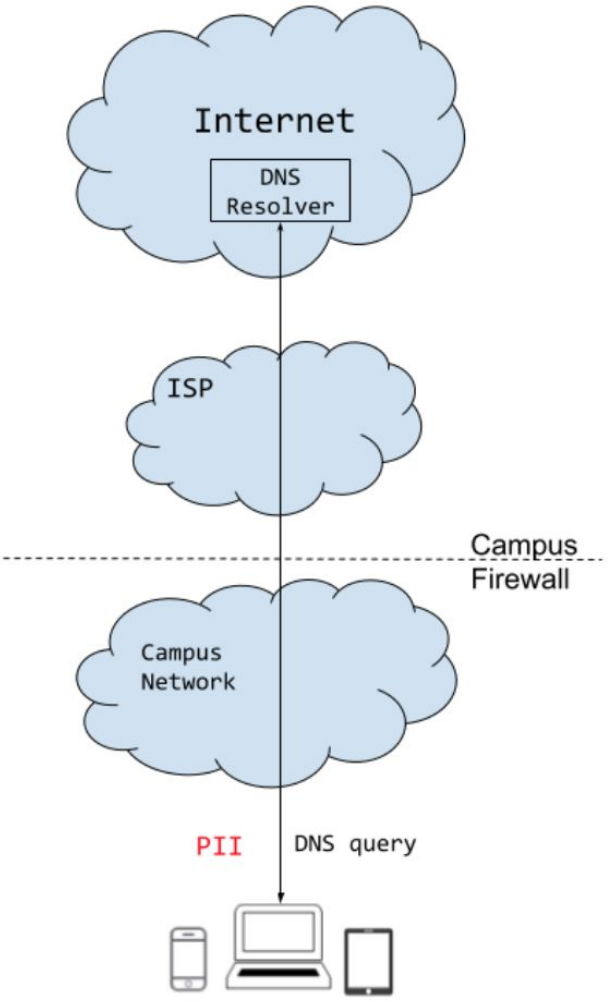
รูปที่ 2 แสดงที่ตั้ง DNS Resolver ณ เครือข่ายคอมพิวเตอร์ของ ISP

ปี 2550 OpenDNS เปิดบริการ DNS Resolver สู่สาธารณะ และพยายามชักจูงให้ผู้ใช้อินเทอร์เน็ตทุกคนใช้งานบริการนี้ โดยชี้ให้เห็นว่าหากใช้บริการ Public DNS Resolver ของ OpenDNS แล้ว ผู้ใช้ทั่วไปจะปลอดภัยมากขึ้น เพราะ OpenDNS จะป้องกันมิให้ผู้ใช้ไปยัง/เข้าถึงเว็บและบริการอื่น ๆ ที่ไม่เหมาะสมบนอินเทอร์เน็ต อีกทั้งหน่วยงานต่าง ๆ จะสามารถควบคุมการเข้าถึงเว็บหรือบริการต่าง ๆ บนอินเทอร์เน็ตของคอมพิวเตอร์ในหน่วยงานของตนได้

อย่างไรก็ตามสิ่งที่ OpenDNS ไม่ได้บอกผู้ใช้งานก็คือ DNS Resolver ของ OpenDNS แอบเปลี่ยนคำตอบของระบบโดเมนเนม โดยการส่งคำค้นหาที่ผู้ใช้ใส่ในช่อง Address Bar ของ Firefox และ IE (เพื่อค้นหาข้อมูลบนอินเทอร์เน็ต) ไปใช้ Search Engine ของ OpenDNS แทน แม้ผู้ใช้จะตั้งค่าในบราวเซอร์ให้ใช้บริการ Search Engine ของ Google ก็ตาม ทาง Google พยายามเจรจากับ OpenDNS แต่การเจรจาไม่เป็นผล ทำให้ในที่สุด Google ต้องตัดสินใจให้บริการ Public DNS Resolver เองในปลายปี พ.ศ. 2551 ประกอบกับในช่วงเดียวกันการใช้งานอินเทอร์เน็ตทั่วโลกเพิ่มขึ้นอย่างมาก แต่ ISP หลายรายไม่มีความสามารถในการดูแล DNS Resolver ของตัวเองให้รองรับกับปริมาณการใช้งาน DNS Resolver ทำให้ลูกค้าของ ISP เปลี่ยนไปใช้ Public DNS Resolver ของ Google ด้วยตนเอง รวมทั้งบาง ISP ก็ลดภาระในการดูแล DNS Resolver ด้วยการกำหนดให้ลูกค้าทุกราย ใช้งาน Public DNS Resolver ของ Google

ต่อมามีบริษัทอีกหลายรายที่เห็นความสำคัญของข้อมูลซึ่งจะได้มาจาก DNS Resolver จึงทยอยเปิดให้บริการ Public DNS resolver เพิ่มขึ้นอีกหลายแห่ง ทำให้ตำแหน่งที่ตั้งของ DNS Resolver เปลี่ยนไปเป็นรูปที่ 3

จากรูปที่ 3 จะเห็นว่าการทำ DNS Query จากอุปกรณ์ของผู้ใช้งานไปยัง DNS Resolver ที่อยู่บนอินเทอร์เน็ตนั้นมีความเสี่ยงที่ข้อมูลส่วนบุคคลจะรั่วไหลมากขึ้นโดยข้อมูลอาจจะรั่วไหลได้จากการแอบสำเนาข้อมูล DNS Query ที่วิ่งผ่านเครือข่ายคอมพิวเตอร์โดยใช้ UDP พอร์ต 53 โดยมิได้รับอนุญาต หรืออาจจะรั่วไหลจากผู้ให้บริการ Public DNS Resolver เองก็ได้ ผู้ใช้บริการที่เป็นหน่วยงาน หรือ ISP ที่ให้บริการหน่วยงานนั้น ๆ ก็ไม่สามารถควบคุมและกำกับดูแลข้อมูลส่วนบุคคลที่เกิดขึ้น ณ Public DNS Resolver ได้



รูปที่ 3 แสดงที่ตั้งของ Public DNS Resolver

ในส่วนประเด็นที่เกี่ยวข้องกับการเก็บข้อมูลส่วนบุคคลนั้น หากผู้ใช้เปลี่ยน DNS Resolver ไปเป็น Public DNS Resolver ด้วยตนเองก็อาจจะกล่าวได้ว่าผู้ใช้รายนั้นให้ความยินยอม (Consent Basis) ที่จะให้ผู้ให้บริการ Public DNS Resolver รายนั้น ๆ ได้ข้อมูลส่วนบุคคลของตนและดำเนินการกับข้อมูลส่วนบุคคลดังกล่าว ตามนโยบายของผู้ให้บริการรายนั้น ๆ แต่หากเป็นกรณีที่ ISP ลดภาระของตนเองโดยการกำหนดให้ลูกค้าของตนไปใช้งาน Public DNS Resolver นั้น ISP รายนั้นอาจเสี่ยงที่จะทำผิดกฎหมาย เพราะมีเจตนาที่จะส่งต่อข้อมูลส่วนบุคคลของลูกค้าไปยังบุคคลที่สาม (ผู้ให้บริการ Public DNS Resolver) โดยไม่ได้แจ้งรายละเอียดและไม่ได้ขอความยินยอมจากลูกค้าของตนเองก่อน หาก Public DNS Resolver นั้นตั้งอยู่ต่างประเทศ ก็จะเข้าข่ายกรณีส่งข้อมูลส่วนบุคคล ไปยังต่างประเทศอีกด้วย

บริการ Public DNS resolver กับประเด็นเรื่องข้อมูลส่วนบุคคลที่ซับซ้อนขึ้น

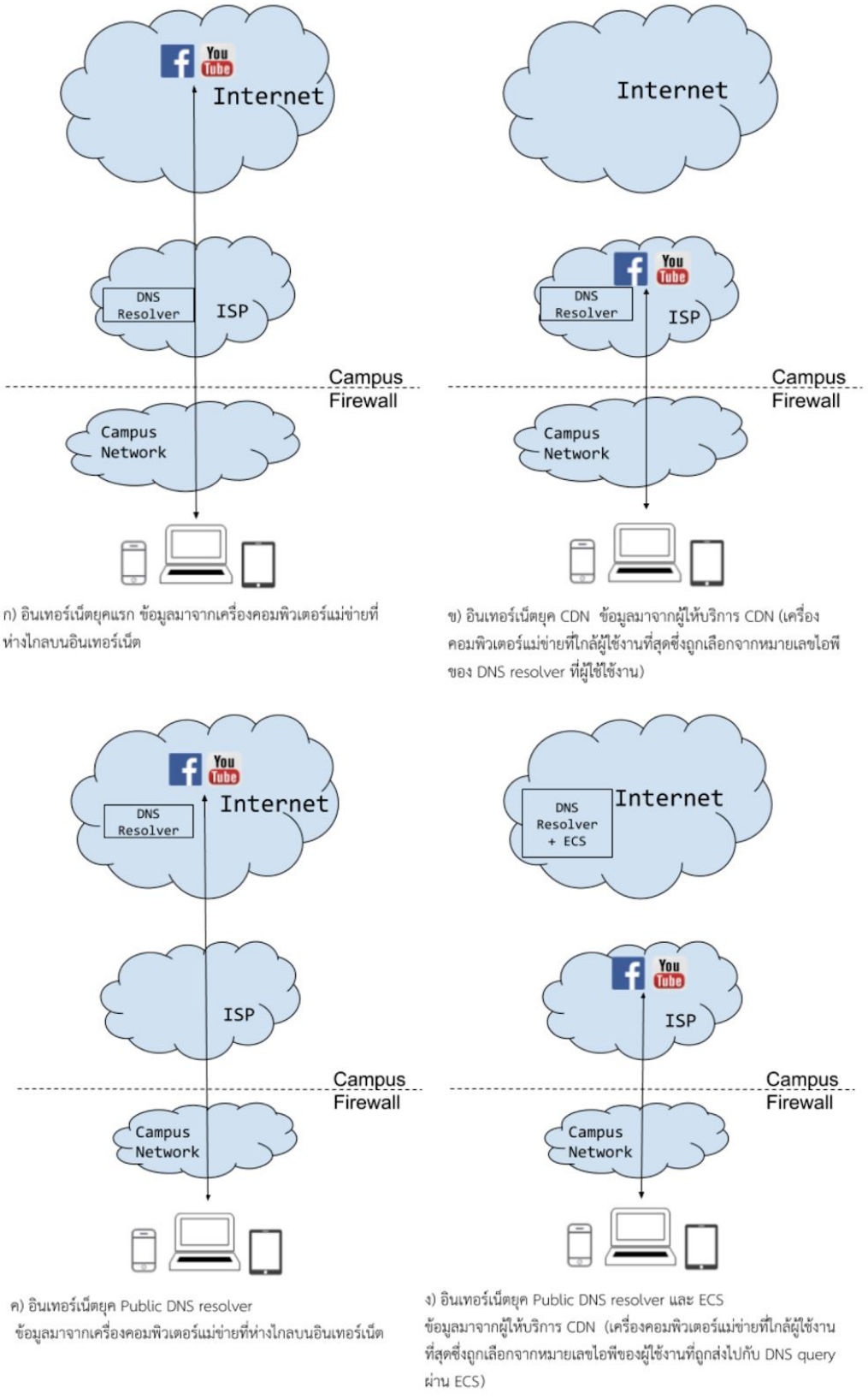
แม้การแก้ปัญหาเฉพาะหน้าของ Google ด้วยการให้บริการ Public DNS Resolver จะแก้ปัญหาการแอบเปลี่ยนคำตอบของ OpenDNS ได้ แต่การแก้ปัญหาด้วยวิธีนี้ก่อให้เกิดปัญหาตามมา 2 ประการ ดังนี้

1. **ปัญหากับผู้ให้บริการ Content Delivery Network (CDN)**

   ผู้ให้บริการ CDN คือผู้ที่ทำหน้าที่ช่วยให้ข้อมูลไปถึงผู้ใช้ปลายทางได้อย่างรวดเร็วและมีประสิทธิภาพ โดยผู้ให้บริการ CDN จะวางเครื่องคอมพิวเตอร์ที่ให้บริการ ข้อมูลกระจายไว้ในภูมิภาคต่าง ๆ ของโลก และจะสำเนาข้อมูลจากต้นทางไปยังคอมพิวเตอร์เหล่านั้น เมื่อผู้ใช้ต้องการข้อมูล DNS Resolver ของผู้ใช้จะสอบถามหมายเลขไอพีของคอมพิวเตอร์ที่เก็บข้อมูลไว้ และเนื่องจากหมายเลขไอพีของ DNS Resolver จะเป็นตัวแทนของเครือข่ายคอมพิวเตอร์ของผู้ใช้ ทำให้ระบบชื่อโดเมนของผู้ให้บริการ CDN ตอบหมายเลขไอพีของคอมพิวเตอร์ที่แตกต่างกันตามหมายเลขไอพีของ DNS Resolver เพื่อให้ผู้ใช้เข้าถึงเครื่องที่เก็บข้อมูลที่อยู่ใกล้ตนเองมากที่สุด แต่เมื่อผู้ใช้บริการอินเทอร์เน็ตเปลี่ยนไปใช้ Public DNS Resolver จึงเกิดผลกระทบกับผู้ให้บริการ CDN อย่างหลีกเลี่ยงไม่ได้ ทำให้เกิดแรงผลักดันในการออกแบบมาตรฐานระบบชื่อโดเมน เพิ่มเติมเพื่อให้ผู้บริการ CDN ทราบว่าผู้ใช้บริการมาจาก ส่วนไหนของอินเทอร์เน็ต ทำให้เกิดส่วนขยายของมาตรฐาน ชื่อโดเมน เรียกว่า EDNS Client Subnet หรือ ECS (RFC 7871) ซึ่งก่อให้เกิดปัญหาใหม่ในเรื่องข้อมูลส่วนบุคคล

2. **ปัญหาเรื่องข้อมูลส่วนบุคคลรั่วไหลที่ต่อมาก่อให้เกิดความขัดแย้งเรื่อง การเข้ารหัสข้อมูล DNS Query**

   ผู้ที่เกี่ยวข้องกับการออกแบบระบบชื่อโดเมนทราบดีว่าข้อมูล DNS Query นั้นเป็นข้อมูลส่วนบุคคลประเภทหนึ่ง เมื่อผู้ใช้เปลี่ยนไปใช้งาน Public DNS Resolver มากขึ้น โอกาสที่ข้อมูลส่วนบุคคลจะรั่วไหลก็มีมากขึ้น ผู้ออกแบบระบบชื่อโดเมนต่างเห็นตรงกันว่าถึงเวลาแล้วที่จะปกป้องข้อมูลส่วนบุคคลของ DNS Query ที่อาจรั่วไหลเพราะการแอบดักจับข้อมูลโดยใช้เทคนิคการเข้ารหัส แต่เกิดความเห็นที่แตกต่างกันในส่วนวิธีการปฏิบัติ จนเกิดแนวทางที่แตกต่างกันเช่น DNScrypt, DNS over Transport Layer Security: DoT (RFC 7858) และ DNS Queries over HTTPS: DoH (RFC 8484)



ก) อินเทอร์เน็ตยุคแรก ข้อมูลมาจากเครื่องคอมพิวเตอร์แม่ข่ายที่ห่างไกลบนอินเทอร์เน็ต

ข) อินเทอร์เน็ตยุค CDN ข้อมูลมาจากผู้ให้บริการ CDN (เครื่องคอมพิวเตอร์แม่ข่ายที่ใกล้ผู้ใช้งานที่สุดซึ่งถูกเลือกจากหมายเลขไอพีของ DNS resolver ที่ผู้ใช้ใช้งาน)

ค) อินเทอร์เน็ตยุค Public DNS resolver ข้อมูลมาจากเครื่องคอมพิวเตอร์แม่ข่ายที่ห่างไกลบนอินเทอร์เน็ต

ง) อินเทอร์เน็ตยุค Public DNS resolver และ ECS ข้อมูลมาจากผู้ให้บริการ CDN (เครื่องคอมพิวเตอร์แม่ข่ายที่ใกล้ผู้ใช้งานที่สุดซึ่งถูกเลือกจากหมายเลขไอพีของผู้ใช้งานที่ถูกส่งไปกับ DNS query ผ่าน ECS)

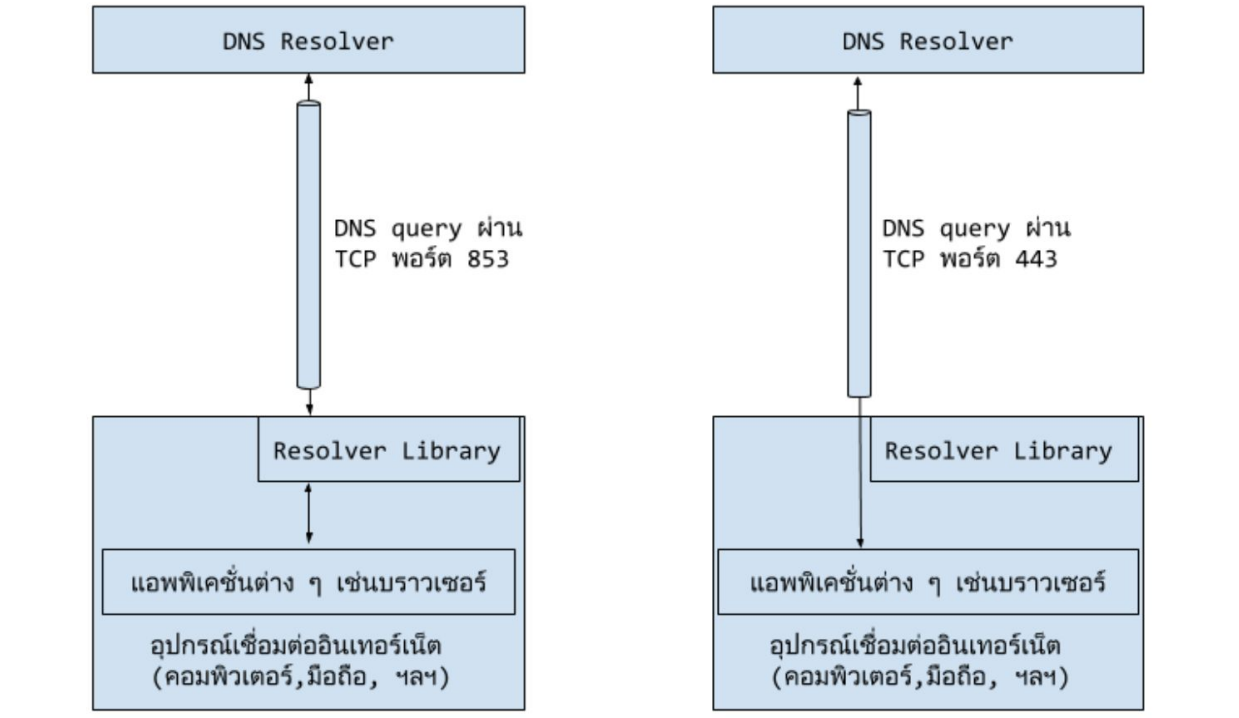
รูปที่ 4 แสดงความสัมพันธ์ระหว่าง DNS Resolver กับบริการ CDN

EDNS Client Subnet ปัญหาข้อมูลส่วนบุคคลที่ซับซ้อนขึ้น

ส่วนขยายเพิ่มเติม EDNS Client Subnet มีไว้เพื่อให้ Authority DNS Server ทราบว่าผู้ใช้บริการมาจากส่วนไหนของอินเทอร์เน็ต เทคนิคที่ EDNS ใช้คือส่งข้อมูลหมายเลขไอพีหรือกลุ่มหมายเลขไอพีของผู้ใช้งานไปยัง Auhority DNS Server ด้วย ทำให้ Authority DNS Server ทราบหมายเลขไอพีหรือกลุ่มของหมายเลขไอพีของผู้ใช้ (เดิมนั้น Authority DNS Server ไม่เคยทราบหมายเลขไอพีหรือ กลุ่มของหมายเลขไอพีของผู้ใช้ จะทราบเฉพาะหมายเลขไอพีของ DNS Resolver เท่านั้น) ปัญหาการรั่วไหลข้อมูลส่วนบุคคลจึงซับซ้อนมากขึ้น

DoT vs DoH ความขัดแย้งที่ยังไม่สิ้นสุด

เทคนิคการเข้ารหัส DNS Query มีหลายวิธีแต่มีเพียง 2 วิธีคือ DoT (DNS over TLS) และ DoH (DNS over HTTPS) ที่ได้รับการยอมรับจนกลายเป็นเอกสาร RFC โดยแม้ DoT และ DoH ใช้การเข้ารหัสเพื่อป้องกันการรั่วไหลของข้อมูลก็ตาม แต่อาศัยแนวทางที่ต่างกันคือ DoT เพิ่มการเข้ารหัสไปที่โครงสร้างเดิมของระบบชื่อโดเมน (แอพพลิเคชั่นเรียกใช้งาน DNS Query ผ่าน Resolver Library ของระบบปฏิบัติการ) แต่ DoH เปลี่ยนโครงสร้างของระบบชื่อโดเมนโดยให้แอพพลิเคชั่นส่ง DNS Query แบบเข้ารหัสตรงไปยัง DNS Resolver โดยไม่ผ่าน Resolver Libary ของระบบปฏิบัติการ ขณะนี้ (มกราคม 2563) แนวทาง DoH อาจจะได้เปรียบเพราะบราวเซอร์รายใหญ่คือ Firefox และ Chrome ต่างก็ใช้งาน DoH ได้แล้ว แต่เนื่องจากแนวทาง DoH เป็นแนวทางที่เปลี่ยนโครงสร้างการทำงานของระบบชื่อโดเมน แนวทางนี้จึงจะสร้างปัญหาใหม่ ๆ ตามมาในอนาคตเป็นจำนวนมาก ส่วนแนวทาง DoT นั้นต้องอาศัยความร่วมมือจากผู้ผลิตระบบปฏิบัติการ ซึ่งขณะนี้มีเพียงบางระบบปฏิบัติการเท่านั้นที่ใช้งาน DoT ได้ เช่น Android 9 หรือ Ubuntu 18.10 เป็นต้น



ก) แนวทางการใช้งาน DNS over TLS (DoT) ข) แนวทางการใช้งาน DNS over HTTPS (DoH)

รูปที่ 5 แสดงโครงสร้างของ DoT และ DoH

แนวทางการใช้งาน DoH ของบราวเซอร์กับข้อมูลส่วนบุคคล

ผู้พัฒนาบราวเซอร์หลายรายสนับสนุนข้อกำหนด DoH (DNS over HTTPS) และปรับปรุงให้บราวเซอร์ของตนเองรองรับ DoH ในรูปแบบที่แตกต่างกันดังนี้

1. **Firefox** บราวเซอร์นี้รองรับ DoH แล้วและได้ตกลงกับบริษัท Cloudfare ให้เป็นผู้ให้บริการ DNS Resolver แบบ DoH ของ Firefox เพียงรายเดียวเรียกว่า Trusted Recursive Resolver (TRR) ผู้พัฒนา firefox วางแผนเปิดการใช้งาน DoH เป็นค่าเริ่มต้นให้กับผู้ใช้งาน Firefox ทั่วโลก โดยเริ่มจากผู้ใช้งาน Firefox ในประเทศสหรัฐอเมริกาเป็นประเทศแรก (ผู้ใช้อาจยกเลิกได้เองแบบ Opt-out) ตั้งแต่เดือนกันยายน 2562 เป็นต้นไป และมีแผนที่จะทยอยเปิดใช้งานไปเรื่อย ๆ อย่างไรก็ตาม หน่วยงานรัฐบาลของประเทศอังกฤษได้เจรจากับผู้พัฒนา Firefox และสั่งห้ามใช้งาน DoH การใช้งาน DoH เป็นค่าเริ่มต้นตามแนวทางของ Firefox จะทำให้ข้อมูลส่วนบุคคลของผู้ใช้งานถูกส่งไปยัง TRR (ผู้ให้บริการ DNS Resolver แบบ DoH) โดยมิได้รับความยินยอมจากผู้ใช้งาน
2. **Chrome** บราวเซอร์ขณะนี้รองรับ DoH แล้ว แต่แนวทางต่างจาก Firefox โดย Chrome จะตรวจสอบว่า DNS Resolver ที่ใช้งานอยู่นั้นเป็น DNS Resolver ที่อยู่ในรายชื่อผู้ให้บริการ DoH (Cleanbrowing, Cloudflare, Comcast, DNS.SB, Google, OpenDNS และ Quad9) หรือไม่ หากพบว่าอยู่ในรายชื่อก็จะทดสอบว่าสามารถใช้บริการ DoH ได้หรือไม่ ถ้าใช้บริการ DoH ได้ก็จะใช้งาน DoH แต่ถ้าใช้บริการไม่ได้ ก็จะใช้งาน DNS แบบปกติ

แนวทางใช้งาน DoH ของ Chrome จะมีประเด็นเรื่องละเมิด ข้อมูลส่วนบุคคลหรือไม่นั้น ขึ้นอยู่กับว่า DNS Resolver ในเครื่องเป็น Public DNS Resolver เพราะผู้ใช้งานกำหนดค่าเอง (ไม่ละเมิด) หรือเพราะ ISP กำหนดค่าให้ (ละเมิด)

3. **Edge** หากใช้ Edge รุ่นล่าสุดที่พัฒนาจาก Chromium จะรองรับการใช้งาน DoH แล้ว แต่ไม่ได้ใช้งาน DoH เป็นค่าเริ่มต้น แต่ผู้ใช้สามารถเลือกใช้เองแบบ Opt-in ได้

4. **Safari** บราวเซอร์นี้ยังไม่รองรับ DoH

สรุป

ทุกคนที่ใช้งานอินเทอร์เน็ตจะต้องใช้งานระบบชื่อโดเมนร่วมด้วยเสมอ และเนื่องจากข้อมูล DNS Query ในระบบชื่อโดเมนเป็นข้อมูลส่วนบุคคล ประเภทหนึ่ง จึงจำเป็นต้องมีการบริหารจัดการที่เหมาะสม ให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ข้อเสนอแนะ

1. ออกข้อกำหนดให้ ISP ต้องจัดให้มีบริการ DNS Resolver ภายในเครือข่ายของตนเอง หาก ISP รายใดต้องการใช้บริการ Public DNS Resolver ISP จะต้องแจ้งเหตุผลความจำเป็น จะต้องแจ้งแนวทางการคุ้มครองข้อมูลส่วนบุคคล และต้องขอความยินยอมจากผู้ใช้งานก่อน
2. เจรจากับผู้พัฒนา Firefox ให้ยกเลิกการใช้งาน DoH เป็นค่าเริ่มต้นสำหรับผู้ใช้งานในประเทศไทย
3. ให้ความรู้กับผู้ใช้งานถึงความเสี่ยงในการละเมิดข้อมูลส่วนบุคคลหากผู้ใช้ตั้งค่า DNS Resolver ให้เป็น Public DNS Resolver
4. ให้หน่วยงานของรัฐและหน่วยงานในกำกับของรัฐใช้งานระบบชื่อ
5. โดเมนของหน่วยงานเอง หรือจากผู้ให้บริการในประเทศเท่านั้น และห้ามไม่ให้หน่วยงานของรัฐและหน่วยงานในกำกับของรัฐใช้บริการระบบชื่อโดเมนจากผู้ให้บริการที่ไม่ได้อยู่ภายในกฎหมายไทย
6. ให้เครื่องคอมพิวเตอร์ที่บุคลากรใด ๆ ใช้ปฏิบัติงานให้หน่วยงานของรัฐและหน่วยงานในกำกับของรัฐใช้งาน ระบบชื่อโดเมนที่ของหน่วยงานนั้นๆ หรือจากผู้ให้บริการที่อยู่ภายใต้กฎหมายไทยเท่านั้น