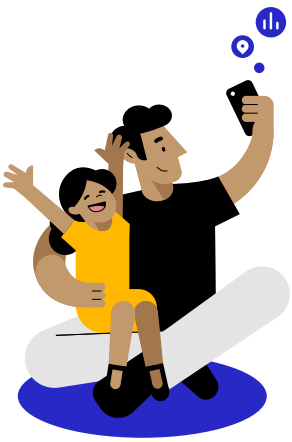


ในหนึ่งวันเกิดอะไรขึ้นกับข้อมูลของคุณบ้าง

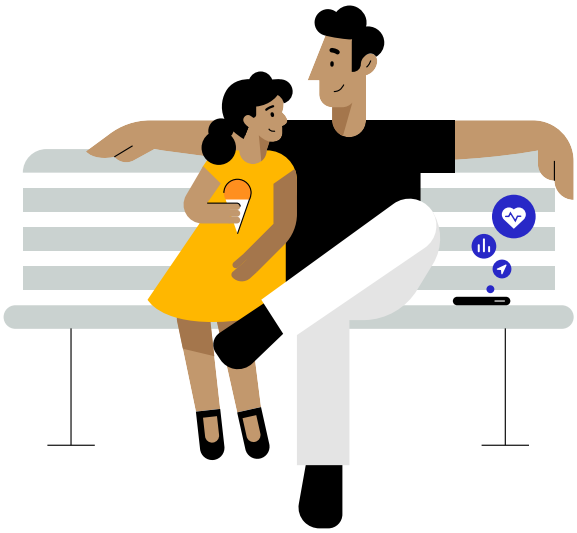
หนึ่งวันของคุณพ่อและลูกสาวที่สนามเด็กเล่น

เมษายน 2021

"ผมเชื่อว่าคนเราฉลาด และบางคนก็อยากแชร์ข้อมูลมากกว่าคนอื่นๆ ดังนั้นเราจึงควรถามถามทุกครั้ง จนกว่าพวกเขาจะเบื่อกับการถูกถามและบอกให้คุณหยุด บอกให้พวกเขารู้อย่างตรงไปตรงมาว่าคุณกำลังจะทำอะไรกับข้อมูลของพวกเขาบ้าง"

Steve Jobs

การประชุม All Things Digital ปี 2010



ในช่วงทศวรรษที่ผ่านมา มีอุตสาหกรรมหนึ่งที่มีขนาดใหญ่และมีความคลุมเครือได้เก็บรวบรวมข้อมูลส่วนตัวมากขึ้นเรื่อยๆ[1,2] เรียกว่าเป็นระบบนิเวศอันซับซ้อนที่ประกอบด้วยเว็บไซต์ แอป บริษัทโซเชียลมีเดีย นายหน้าหาข้อมูล และบริษัทเทคโนโลยีโฆษณาต่างคอยติดตามผู้ใช้ทั้งทางออนไลน์และออฟไลน์เพื่อเก็บเกี่ยวข้อมูลส่วนตัวของผู้ใช้ โดยข้อมูลเหล่านี้ได้ถูกนำมาปะติดปะต่อ แชร์ รวมเข้าด้วยกัน และใช้ในการประมูลแบบเรียลไทม์ เพื่อหล่อเลี้ยงอุตสาหกรรมที่มีมูลค่าสูงถึง 2.27 แสนล้านดอลลาร์ต่อปี[1] สิ่งที่ว่านี้ยังเกิดขึ้นทุกวันในขณะที่ผู้คนใช้ชีวิตประจำวัน และบ่อยครั้งมักจะเกิดขึ้นโดยที่พวกเขาไม่ได้รับรู้หรืออนุญาตเลยด้วยซ้ำ[3,4] ถ้าเป็นอย่างนั้น เรามาลองดูกันว่าอุตสาหกรรมนี้สามารถล่วงรู้อะไรได้บ้างเกี่ยวกับคุณพ่อและลูกสาวคู่หนึ่งที่ควรจะได้ใช้เวลาร่วมกันที่สวนสาธารณะอย่างมีความสุขหากไม่เกิดเหตุการณ์ดังกล่าวขึ้น

รู้หรือไม่

แอปที่คุณใช้อยู่เป็นประจำทุกวันมีตัวติดตามฝังอยู่ ซึ่งโดยเฉลี่ยแล้วในหนึ่งแอปจะมีตัวติดตาม 6 ตัว[3] และแอปยอดนิยมส่วนใหญ่ของทั้ง Android และ iOS นั้นมีตัวติดตามฝังอยู่[5,6,7]

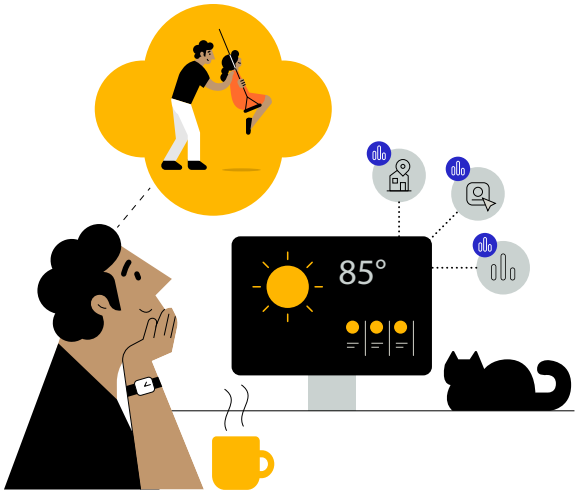
ตัวติดตามมักถูกฝังอยู่ในโค้ดของบริษัทอื่นที่ช่วยนักพัฒนาในการสร้างแอป และการที่นักพัฒนาใส่ตัวติดตามเหล่านี้ไว้ก็ยังช่วยให้บริษัทอื่นสามารถเก็บรวบรวมและเชื่อมโยงข้อมูลที่คุณแชร์กับบริษัทเหล่านั้นข้ามไปมาระหว่างแอป และนำไปเชื่อมโยงกับข้อมูลอื่นๆ เกี่ยวกับตัวคุณที่มีการเก็บไว้ได้

นายหน้าหาข้อมูลหรือ Data Broker เป็นผู้เก็บรวบรวมและจำหน่ายให้สิทธิ์ใช้งาน หรือเปิดเผยข้อมูลส่วนตัวต่างๆ กับบริษัทอื่น โดยที่ข้อมูลนั้นเป็นของบุคคลใดบุคคลหนึ่งที่บริษัทไม่ได้มีความสัมพันธ์โดยตรงแต่อย่างใด[3]

นายหน้าหาข้อมูลหลายร้อยรายเก็บข้อมูลทั้งทางออนไลน์และออฟไลน์[8] และนายหน้ารายหนึ่งเก็บข้อมูลจากผู้ใช้งานทั่วโลก 700 ล้านคน แล้วนำมาสร้างเป็นโปรไฟล์ของผู้ใช้งานที่มีลักษณะเฉพาะตัวได้สูงสุดถึง 5,000 รายการ[9]

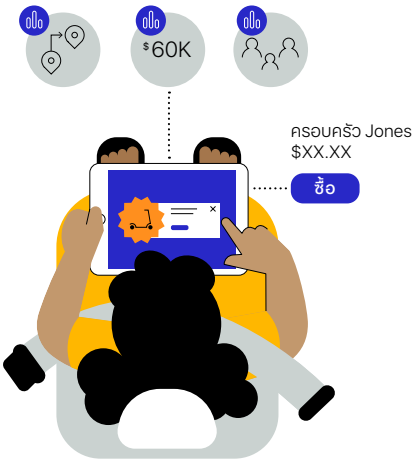
จากการศึกษาพบว่าในแอปสำหรับเด็กเกือบ 20% นั้น นักพัฒนามีการเก็บและแชร์ข้อมูลที่สามารถระบุตัวตนของบุคคลได้ โดยไม่ได้รับความยินยอมจากผู้ปกครอง[10]

ในแต่ละชั่วโมงของแต่ละวัน มีการแสดงโฆษณาดิจิทัลหลายพันล้านตัวให้ผู้ใช้เห็นทางออนไลน์[11,12,13] และในเวลาเพียงเสี้ยววินาทีที่ใช้ในการโหลดโฆษณานั้น ก็มีการประมูลเกิดขึ้นไปพร้อมๆ กัน โดยผู้โฆษณาจะเสนอราคาเพื่อซื้อพื้นที่โฆษณาดังกล่าว และบ่อยครั้งที่มักอาศัยข้อมูลส่วนตัวที่มีการติดตามเกี่ยวกับบุคคลนั้นด้วย[14,15]



John วางแผนว่าจะพาลูกสาวไปสวนสาธารณะ

วันนี้ John กับ Emma ลูกสาววัย 7 ขวบ ใช้เวลาอยู่ด้วยกัน โดยในตอนเช้า John ใช้คอมพิวเตอร์เช็คสภาพอากาศ อ่านข่าว และเปิดแอปแผนที่บนสมาร์ทโฟนเพื่อดูสภาพการจราจรของเส้นทางไปยังสนามเด็กเล่นที่อยู่ติดกับโรงเรียนของลูกสาว ซึ่งในระหว่างทางนั้นมีแอป 4 แอปบนโทรศัพท์กำลังเก็บและติดตามข้อมูลตำแหน่งของพวกเขาเป็นระยะๆ อยู่ในเบื้องหลัง[16,17,18] โดยหลังจากดึงข้อมูลที่ต้องการจากอุปกรณ์ได้แล้ว นักพัฒนาแอปก็จะขายข้อมูลนั้นให้กับบริษัทอื่นอีกหลายรายที่เป็นนายหน้าหาข้อมูลซึ่ง John ไม่เคยรู้จักมาก่อน[16,17] และถึงแม้จะอ้างว่าข้อมูลบอกตำแหน่งที่เก็บไปนั้นไม่ระบุตัวตน แต่การติดตามผู้ใช้ก็ทำให้นายหน้าหาข้อมูลสามารถเชื่อมโยงสถานที่ที่ John เคยไปจากแอปเหล่านี้กับข้อมูลที่เก็บไว้ขณะที่เขาใช้แอปอื่นๆ ได้[16,19] นั่นหมายความว่าบริษัทและองค์กรใดก็ตามสามารถหาซื้อข้อมูลที่มีการติดตามข้ามแอปและข้อมูลจากแหล่งอื่นๆ เพื่อนำไปใช้สร้างโปรไฟล์ที่มีข้อมูลครบถ้วนเกี่ยวกับตัวเขาได้ รวมถึงการเคลื่อนไหวของเขาในแต่ละวันชนิดที่ตามติดทุกย่างก้าว[3,16]



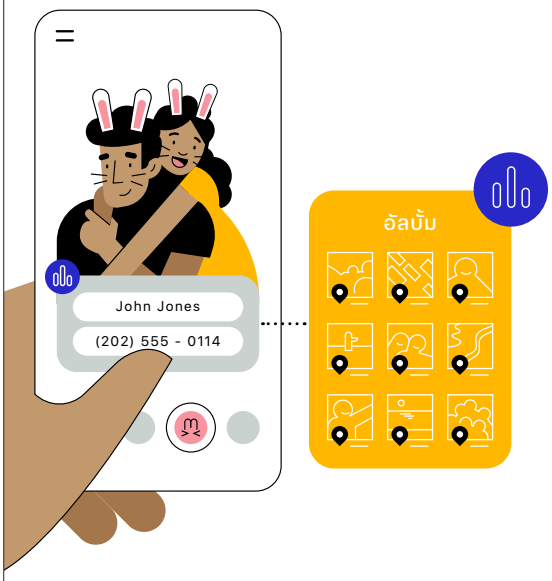
Emma เล่นเกมระหว่างทางไปสวนสาธารณะ

ระหว่างทางไปสนามเด็กเล่น John ให้ลูกสาวเล่นเกมบนแท็บเล็ต และเมื่อเธอเปิดแอป เธอก็เห็นโฆษณารถสกูตเตอร์ ซึ่งบอกเลยว่าไม่ใช่เรื่องบังเอิญ เพราะในเวลาเพียงเสี้ยววินาทีที่โหลดแอป ก็มีการประมูลพื้นที่โฆษณานั้นเกิดขึ้นแล้ว[14] เริ่มจากการที่บริษัทโฆษณาซึ่งทำหน้าที่ในนามของบริษัทรถสกูตเตอร์ ทราบข้อมูลจากบริษัทที่เป็นคนกลางว่ามีพื้นที่โฆษณาว่าง[15] บริษัทจึงเสนอราคาเพื่อซื้อพื้นที่โฆษณานั้นโดยอาศัยข้อมูลส่วนตัวเกี่ยวกับ John และ Emma ที่เก็บไว้[15] จากนั้นพันธมิตรโฆษณาของบริษัทรถสกูตเตอร์ก็ยังคงเก็บข้อมูลเกี่ยวกับพฤติกรรมของ John และ Emma หลังจากที่เห็นโฆษณานั้นต่อไป เพื่อดูว่าทั้งสองคนคลิกโฆษณาหรือซื้อรถสกูตเตอร์หรือไม่[3] ซึ่งบริษัทก็จะโฆษณารถสกูตเตอร์ให้ John และ Emma ต่อไปเรื่อยๆ ในทุกช่องทางเท่าที่จะทำได้โดยการติดตามข้ามไปยังแอปและเว็บไซต์ต่างๆ บนอุปกรณ์ทุกเครื่องของ John[3,20,21]

มีบางแอปขอเข้าถึงข้อมูลมากกว่าที่จำเป็นต้องใช้ในการให้บริการ เช่น เป็นแอปประเภทคีย์บอร์ดแต่ขอเข้าถึงตำแหน่งที่แน่นอนของผู้ใช้[5]

ข้อมูลที่แลกเปลี่ยนกันนั้นอาจไปอยู่ที่เครือข่ายโฆษณา ผู้เผยแพร่โฆษณา ผู้ให้บริการด้านการระบุที่มาและวัดผลโฆษณา นายหน้าหาข้อมูล บริษัทเอกชนอื่นๆ หรือแม้แต่หน่วยงานของรัฐ[3,15,40,41,42] ซึ่งบริษัทโซเชียลมีเดียและเทคโนโลยีโฆษณาต้องเจอหรือเสียค่าปรับไปแล้วหลายล้านดอลลาร์จากการใช้ข้อมูลส่วนตัวเพื่อจุดประสงค์อื่นนอกเหนือจากที่เคยแจ้งให้ผู้ใช้ทราบเมื่อตอนที่มีการเก็บข้อมูล[22,23,24,25]

นายหน้าหาข้อมูลใช้ข้อมูลที่เก็บมาในการกำหนดลักษณะเฉพาะให้กับผู้ใช้แล้วนำมาจัดแบ่งออกเป็นเซกเมนต์ตลาดต่างๆ แบบละเอียดยิบ ตัวอย่างเช่นผู้ที่ "กำลังพยายามลดน้ำหนักแต่ยังชอบทานเบเกอรี่"[26] แต่โปรไฟล์เหล่านี้มักจะผิด เพราะจากการศึกษาพบว่าลักษณะเฉพาะเหล่านี้กว่า 40% ไม่ตรงกับความเป็นจริง[27,28]

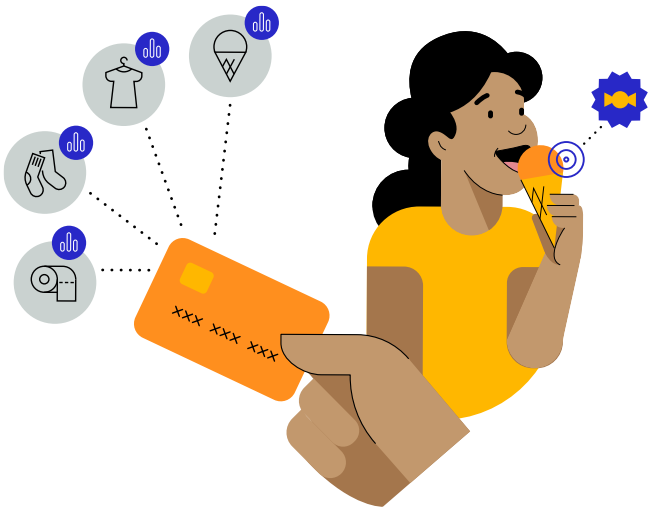


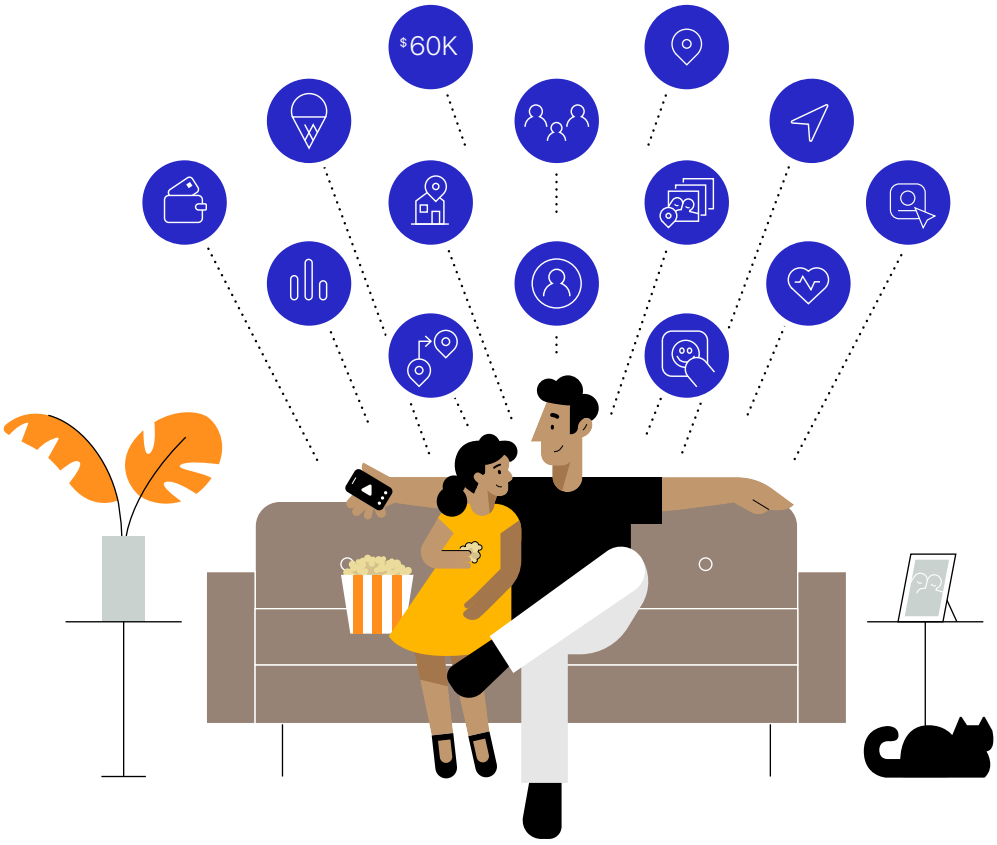
John และ Emma ถ่ายเซลฟี่ที่สวนสาธารณะ

ต่อมาขณะอยู่ที่สนามเด็กเล่น John และ Emma ถ่ายเซลฟี่ด้วยกัน จากนั้นก็ลองเล่นแอปสำหรับใส่ฟิลเตอร์ให้รูปถ่าย ซึ่งทั้งคู่ตกลงเลือกใส่หูกระต่ายลงในรูป แต่ผลลัพธ์ไม่ใช่แค่นั้น เพราะแทนที่แอปใส่ฟิลเตอร์จะเข้าถึงแค่เฉพาะภาพเซลฟี่ที่สนามเด็กเล่น กลับกลายเป็นว่าแอปสามารถเข้าถึงรูปภาพทั้งหมดบนอุปกรณ์ รวมถึงเมตาดาต้าที่มาพร้อมรูปเหล่านั้นได้[29,30] ซึ่งเมื่อ John โพสต์รูปลงบนแอปโซเชียลมีเดีย แอปก็ทำการเชื่อมโยงกิจกรรมออนไลน์ของ John ในขณะนั้นเข้ากับข้อมูลอีกมากมายที่เก็บโดยแอปอื่นๆ อย่างข้อมูลทางประชากรศาสตร์และลักษณะนิสัยในการซื้อสินค้าของเขา โดยใช้เพียงแค่ที่อยู่อีเมล หมายเลขโทรศัพท์ หรือข้อมูลโฆษณาประจำตัว[3]

แวะทานไอศกรีมระหว่างทางกลับบ้าน

ระหว่างทางกลับบ้าน John และ Emma แวะทานไอศกรีม โดย John ได้ใช้บัตรเครดิตจ่ายค่าไอศกรีม นั่นหมายความว่ามีการเพิ่มข้อมูลนั้นลงในโปรไฟล์ที่มีรายละเอียดเกี่ยวกับสิ่งที่เขาชอบอย่างครบถ้วน ไม่ว่าจะเป็นตำแหน่งที่ตั้งของร้าน และยอดใช้จ่าย[31,32,33] ขณะเดียวกันอีกแอปหนึ่งที่ติดตามตำแหน่งของ John ยังสังเกตเห็น John กับ Emma หยุดแวะที่ร้านของเล่นด้วย[3] แน่นอนว่าข้อมูลเกี่ยวกับร้านที่ครอบครัวนี้ชื่นชอบในวันนั้นก็ถูกส่งต่อไปยังนายหน้าหาข้อมูล ซึ่งนำข้อมูลดังกล่าวไปรวมกับสิ่งที่รู้อยู่แล้วว่าเขามีลูกที่ยังเด็ก จากนั้นจึงระดมยิงโฆษณาแบบเจาะจงเป้าหมายไปยังอุปกรณ์ของ John ทั้งโฆษณาของหวานและร้านของเล่นที่พวกเขาแวะไป[17]





เมื่อจบวัน หลายบริษัททั่วโลกที่ John ไม่เคยโต้ตอบด้วยเลยต่างก็พากันอัปเดตข้อมูลในโปรไฟล์เกี่ยวกับตัวเขาและลูกสาว กลายเป็นว่าบริษัทเหล่านี้รู้ทั้งตำแหน่งที่อยู่บ้านของครอบครัว สวนสาธารณะที่พวกเขาไป เว็บไซต์ข่าวที่อ่าน ผลิตภัณฑ์ที่เลือกชม โฆษณาที่ดู ลักษณะนิสัยในการซื้อสินค้า และร้านที่ไป[3,34] เพราะข้อมูลเหล่านี้ถูกเก็บและติดตามข้ามแอปต่างๆ ที่ John และลูกสาวใช้งานตลอดทั้งวัน รวมถึงจากแหล่งอื่นๆ ด้วย โดยที่ John ไม่รู้เลยว่ามีการเก็บข้อมูลไปมากแค่ไหนตลอดวันนั้น อีกทั้งยังไม่สามารถควบคุมเรื่องนี้ได้ทุกครั้ง หรือไม่รู้ตัวเลยด้วยซ้ำว่าเคยอนุญาตไปเมื่อไหร่[3,4] ซึ่งเมื่อสองพ่อลูกกลับมาพักผ่อนที่บ้านในตอนเย็นแล้วค้นหาภาพยนตร์สำหรับเด็กในแอปบนสมาร์ททีวี วงจรการติดตาม การแลกเปลี่ยนข้อมูล การประมูล และการย้ำกลุ่มเป้าหมายนั้นก็ยังคงวนเวียนต่อไปไม่จบสิ้น[35,36]

ดูเพิ่มเติมเกี่ยวกับคุณสมบัติด้านความเป็นส่วนตัวที่ Apple ได้เปิดตัวไป รวมถึงสิ่งที่ Apple กำลังทำอยู่เพื่อปกป้องความเป็นส่วนตัวของผู้ใช้ที่ **apple.com/th/privacy**

ดูเพิ่มเติมว่า Safari ปกป้องความเป็นส่วนตัวของคุณอย่างไร อ่านได้ใน **รายงานอย่างเป็นทางการเกี่ยวกับ Safari**

ดูเพิ่มเติมว่า Apple ปกป้องข้อมูลบอกตำแหน่งของคุณอย่างไร อ่านได้ใน **รายงานอย่างเป็นทางการเกี่ยวกับบริการหาตำแหน่งที่ตั้ง**

หลักการด้านความเป็นส่วนตัวของ Apple

Apple เชื่อว่าความเป็นส่วนตัวคือสิทธิมนุษยชนขั้นพื้นฐาน เราจึงออกแบบผลิตภัณฑ์และบริการของเราโดยยึดตามหลักการด้านความเป็นส่วนตัว 4 ข้อหลักของเราดังนี้

การลดปริมาณข้อมูลให้เหลือน้อยที่สุด
เก็บข้อมูลให้น้อยที่สุดเท่าที่จำเป็นต้องใช้ในการตอบสนองสิ่งที่คุณต้องการสำหรับบริการนั้นๆ

การประมวลผลบนอุปกรณ์
ประมวลผลข้อมูลบนอุปกรณ์ทุกครั้งที่ทำได้ แทนการส่งข้อมูลไปยังเซิร์ฟเวอร์ของ Apple ทั้งนี้ก็เพื่อปกป้องความเป็นส่วนตัวของผู้ใช้และลดการเก็บข้อมูลให้น้อยที่สุดนั่นเอง

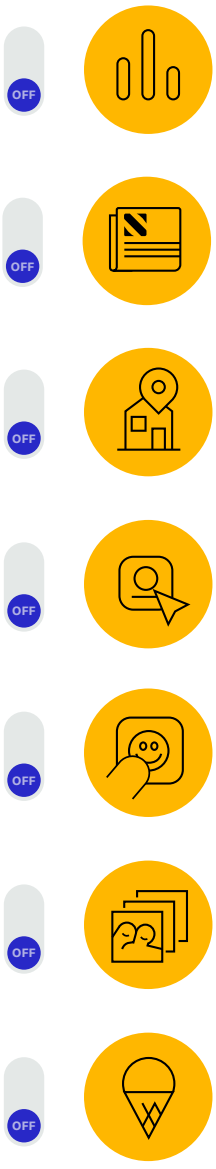
ความโปร่งใสและการควบคุมสำหรับผู้ใช้
แจ้งให้ผู้ใช้ทราบทุกครั้งว่ามีการแชร์ข้อมูลอะไรบ้าง มีการนำข้อมูลนั้นไปใช้อย่างไร และผู้ใช้สามารถควบคุมเรื่องดังกล่าวได้

ความปลอดภัย
ฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกันเพื่อปกป้องข้อมูลให้ปลอดภัยอยู่เสมอ

เป้าหมายของ Apple ซึ่งอาศัยหลักการ 4 ข้อข้างต้น คือการเปิดโอกาสให้ผู้ใช้แชร์ข้อมูลได้เท่าที่ต้องการมาโดยตลอด ด้วยวิธีที่ปลอดภัยโดยที่ผู้ใช้เข้าใจและควบคุมได้ และนี่คือเหตุผลที่ว่าทำไมในช่วงสองทศวรรษที่ผ่านมานี้ Apple จึงไม่เคยหยุดสร้างนวัตกรรมเพื่อปกป้องความเป็นส่วนตัวของผู้ใช้ผ่านผลิตภัณฑ์และบริการของเรา ตัวอย่างเช่น เราใช้ระบบอัจฉริยะบนอุปกรณ์และคุณสมบัติอื่นๆ เพื่อลดปริมาณข้อมูลที่มีการเก็บในแอปเบราว์เซอร์ และบริการออนไลน์ของเราให้เหลือน้อยที่สุด ที่สำคัญคือไม่ว่าจะเป็นแอปหรือบริการไหนๆ ของเราก็จะไม่มีการสร้างโปรไฟล์ที่รวมข้อมูลทั้งหมดของผู้ใช้ไว้อย่างละเอียดในที่เดียวแน่นอน

คุณสมบัติด้านความเป็นส่วนตัวของ Apple ช่วยเพิ่มความโปร่งใสและทำให้ John สามารถควบคุมข้อมูลของตนเองได้ดียิ่งขึ้น

เรื่องราวในหนึ่งวันของ John และ Emma แสดงให้เห็นถึงปัญหาด้านความเป็นส่วนตัวและทางออกที่พวกเราที่ Apple กำลังมุ่งพัฒนาอยู่



John วางแผนว่าจะพาลูกสาวไปสวนสาธารณะ

หาก John ใช้เบราว์เซอร์ Safari เพื่อเช็คสภาพอากาศบนคอมพิวเตอร์ คุณสมบัติ "การป้องกันการติดตามอัจฉริยะ" ก็คงช่วยป้องกันไม่ให้มีการติดตามการใช้งานนี้ ตั้งแต่เริ่มต้นได้

หาก John ใช้ Apple News เพื่ออ่านข่าวในตอนเช้า Apple ก็คงสามารถแสดงเนื้อหาตามความสนใจของ John ได้โดยไม่ต้องรู้ว่าเขาเป็นใครหรืออ่านอะไร

หาก John ใช้แอปแผนที่ของ Apple เพื่อตรวจสอบสภาพการจราจร ข้อมูลบอกตำแหน่งของเขาก็คงเชื่อมโยงกับตัวระบุแบบสุ่ม ซึ่งมีการรีเซ็ตอยู่เป็นระยะๆ และไม่เชื่อมโยงกับ John เพียงเท่านี้ก็จะไม่มีใครนอกจาก John ที่รู้ตำแหน่งของตัวเอง

หาก John ใช้ iPhone ก็คงได้รับการเตือนอยู่เป็นระยะๆ ว่ามีแอปใดบ้างที่กำลังเข้าถึงตำแหน่งของเขาอยู่ในเบื้องหลัง และก่อนแชร์ตำแหน่งกับแอป John ก็สามารถเลือกแชร์เฉพาะตำแหน่งแบบคร่าวๆ หรือแชร์ตำแหน่งเพียงแค่ครั้งเดียวก็ได้

Emma เล่นเกมระหว่างทางไปสวนสาธารณะ

หากเป็น iPad คุณสมบัติ “ความโปร่งใสในการติดตามของแอป” ซึ่งจะพร้อมใช้งานในเร็ววันนี้คงเปิดโอกาสให้ John เลือกว่า จะอนุญาตให้เกมติดตามการใช้งานของ Emma ข้ามไปยังแอปและเว็บไซต์ที่เป็นของบริษัทอื่นหรือไม่

และเครือข่ายโฆษณาที่ใช้ SKAdNetwork API ของ Apple ก็คงจะสามารถวัดประสิทธิภาพโดยรวมของโฆษณาได้โดยไม่ต้องเข้าถึงข้อมูลที่อาจสืบย้อนกลับมาที่อุปกรณ์ของ John ได้

John และ Emma ถ่ายเซลฟี่ที่สวนสาธารณะ

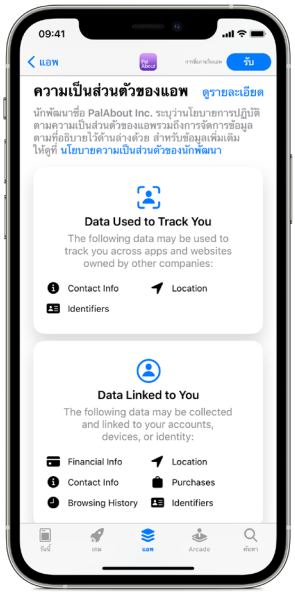
หาก John ใช้ iPhone ก็คงสามารถเลือกได้ว่าต้องการให้แอปฟิลเตอร์เข้าถึงเฉพาะภาพเซลฟี่นั้นแทนที่จะเข้าถึงทั้งคลังรูปภาพ

แวะทานไอศกรีมระหว่างทางกลับบ้าน

หาก John ซื้อไอศกรีมโดยใช้ Apple Card ธนาคารก็คงไม่ใช้ข้อมูลการทำธุรกรรมของเขาเพื่อจุดประสงค์ด้านการตลาด และหากเขาใช้ Apple Pay ทาง Apple ก็คงใช้ระบบอัจฉริยะบนอุปกรณ์เพื่อให้ John สามารถดูประวัติการทำธุรกรรมของตัวเองบน iPhone ได้โดยที่ Apple ไม่ต้องขอข้อมูลเกี่ยวกับสถานที่ที่เขาซื้อสินค้า สิ่งที่ซื้อ หรือยอดใช้จ่าย

เมื่อจบวัน ผลิตภัณฑ์และคุณสมบัติด้านความเป็นส่วนตัวของ Apple สามารถช่วยเพิ่มความโปร่งใสและทำให้ John ควบคุมได้ดียิ่งขึ้นตลอดทั้งวันว่ามีการแชร์ข้อมูลของเขามากแค่ไหน และมีการนำข้อมูลนั้นไปใช้อย่างไรบ้าง

ความโปร่งใสในการติดตามของแอปและส่วนใหม่ใน App Store เกี่ยวกับข้อมูลความเป็นส่วนตัว



Apple กำลังก้าวสู่ขั้นตอนต่อไปในการปกป้องความเป็นส่วนตัวของผู้ใช้ภายในระบบนิเวศของแอป ซึ่งในฐานะของกลุ่มองค์กรที่มีโครงสร้างซับซ้อนและกำลังเติบโต อีกทั้งยังเป็นผู้ที่เข้าถึง ติดตาม และสร้างรายได้จากข้อมูลส่วนบุคคลของผู้บริโภค Apple จึงตั้งใจที่จะเปิดใช้งานคุณสมบัติใหม่ 2 รายการที่มีจุดประสงค์เพื่อเพิ่มความโปร่งใส ความชัดเจน และทางเลือกเพื่อให้ผู้ใช้มีข้อมูลประกอบการตัดสินใจที่ครบถ้วน และควบคุมความเป็นส่วนตัวของตนเองได้มากยิ่งขึ้น

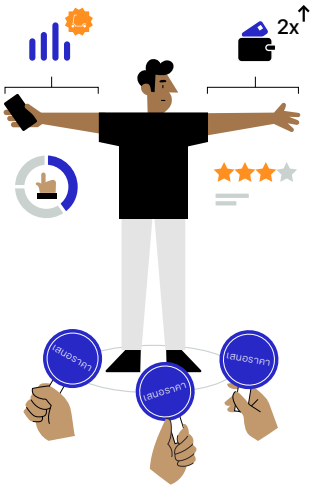
ในอีกไม่นาน คุณสมบัติ "ความโปร่งใสในการติดตามของแอป" ซึ่งจะมาพร้อมกับการอัปเดตรุ่นเบต้าครั้งต่อไป จะกำหนดให้แอปต้องขออนุญาตผู้ใช้ก่อนที่จะติดตามข้อมูลของผู้ใช้ข้ามไปยังแอปหรือเว็บไซต์ของบริษัทอื่น และผู้ใช้ยังสามารถเข้าไปที่การตั้งค่าเพื่อดูว่ามีแอปใดบ้างที่ขออนุญาตติดตาม ซึ่งสามารถปรับเปลี่ยนเองได้ตามความเหมาะสม โดยข้อกำหนดนี้จะเริ่มมีผลเป็นวงกว้างพร้อมกับ iOS 14, iPadOS 14 และ tvOS 14 เวอร์ชั่นต่อไป ซึ่งเป็นเรื่องที่ได้รับการสนับสนุนเป็นอย่างดีจากหน่วยงานที่ส่งเสริมด้านความเป็นส่วนตัวทั่วโลก และเหตุผลที่ Apple ออกแบบคุณสมบัตินี้ก็เพื่อต้องการเพิ่มความโปร่งใสและช่วยให้ผู้ใช้ควบคุมได้มากขึ้นโดยที่ยังคงเปิดให้มีการโฆษณาต่อไปได้เช่นเดิม เนื่องจากโฆษณาเองก็เป็นวิธีการสนับสนุนแอปและเว็บคอนเทนต์ที่พึงกระทำได้และมีความเหมาะสม ซึ่งการเปิดตัวคุณสมบัติที่ผ่านมาอย่าง "การป้องกันการติดตามอัจฉริยะ" ของ Safari ก็ได้แสดงให้เห็นแล้วว่าโฆษณายังคงประสบความสำเร็จได้เช่นเดิม และในขณะเดียวกันยังปกป้องความเป็นส่วนตัวของผู้ใช้ได้ดียิ่งขึ้นด้วย และจนถึงวันนี้คุณสมบัติ "ความโปร่งใสในการติดตามของแอป" ก็ช่วยให้ผู้ใช้มีข้อมูลประกอบการตัดสินใจที่ครบถ้วนเกี่ยวกับแอปที่ใช้ รวมถึงสิ่งที่อนุญาตให้แอปเหล่านั้นทำได้ และคุณสมบัติ "ความโปร่งใสในการติดตามของแอป" ยังช่วยให้ผู้ใช้สามารถเลือกได้ว่าจะอนุญาตให้แอปติดตามหรือไม่ ซึ่งสำหรับแอปที่ผู้ใช้เชื่อถือและอนุญาตให้ติดตามนั้น นักพัฒนาก็สามารถปฏิบัติเช่นเดิมต่อไปได้

นอกเหนือจากการกำหนดให้ต้องขออนุญาตผู้ใช้ก่อนติดตามแล้ว เมื่อไม่นานมานี้ Apple ยังได้ปรับเปลี่ยนหน้าผลิตภัณฑ์ใน App Store เพื่อเพิ่มความโปร่งใสอีกด้วย นั่นก็คือส่วนข้อมูลความเป็นส่วนตัวของแอปที่เพิ่มมาใหม่ใน App Store ที่จะช่วยให้ผู้ใช้เข้าใจแนวทางด้านความเป็นส่วนตัวของแอปนั้นได้ดียิ่งขึ้น โดยหน้าผลิตภัณฑ์ของแต่ละแอปจะต้องแสดงข้อมูลสรุปที่อ่านง่ายเกี่ยวกับแนวทางด้านความเป็นส่วนตัวของนักพัฒนาให้ผู้ใช้ทราบ และในหน้ารายละเอียดจะแสดงข้อมูลเกี่ยวกับประเภทของข้อมูลที่แอปนั้นเก็บ เช่น รูปภาพ ตำแหน่ง และข้อมูลการติดต่อ ยิ่งไปกว่านั้น หน้านี้ยังแสดงรายละเอียดเพิ่มเติมให้ผู้ใช้ทราบด้วยว่านักพัฒนาแอปจะนำข้อมูลแต่ละประเภทไปใช้อย่างไรบ้าง อย่างเช่นว่ามีการใช้ข้อมูลนั้นเพื่อการติดตามหรือไม่ หรือมีการเชื่อมโยงข้อมูลนั้นกับผู้ใช้หรือไม่ ซึ่งการรายงานข้อมูลเกี่ยวกับแนวทางด้านความเป็นส่วนตัวด้วยตนเองนั้นก็ถือเป็นข้อกำหนดที่นักพัฒนาแอปทุกรายต้องปฏิบัติตาม รวมถึง Apple เองด้วย

การเพิ่มมาของการตั้งค่าด้านการติดตามของแอปและความโปร่งใส รวมถึงข้อมูลความเป็นส่วนตัวใน App Store ช่วยเสริมให้ผู้ใช้ทราบได้ง่ายขึ้นว่ามีการนำข้อมูลส่วนตัวไปใช้อย่างไรบ้าง เรียกได้ว่าเป็นการเผยให้เห็นแนวทางปฏิบัติซึ่งครั้งหนึ่งเคยเป็นเรื่องที่ถูกปิดบังและคลุมเครือ และทำให้ผู้ใช้สามารถควบคุมข้อมูลของตนเองได้ดียิ่งขึ้น

Apple จะยังคงเดินหน้าพัฒนาเทคโนโลยีด้านความเป็นส่วนตัวอันล้ำสมัยต่อไป พร้อมกับคิดหาวิธีใหม่ๆ ในการปกป้องดูแลข้อมูลส่วนตัวของคุณให้ปลอดภัยอยู่เสมอ

ในหนึ่งวันเกิดอะไรขึ้นกับโฆษณาบ้าง



การประมูลโฆษณา

การที่ Emma เห็นโฆษณารถสกูตเตอร์บนหน้าจอของ John ไม่ใช่เรื่องบังเอิญ แต่เป็นเพราะมีผู้โฆษณาเสนอราคาในการประมูลเพื่อแสดงโฆษณาบนอุปกรณ์เครื่องดังกล่าว[37] ซึ่งเราจะอธิบายให้คุณเข้าใจง่ายๆ ว่าภายในเสี้ยววินาที มีการเลือกโฆษณาที่จะปรากฏบนหน้าจอของอุปกรณ์อย่างไร

1.
นักพัฒนาแอปที่ Emma ใช้งาน จ้างบริษัทเทคโนโลยีโฆษณาให้ทำหน้าที่ประมูลพื้นที่โฆษณาแบบเรียลไทม์[14]

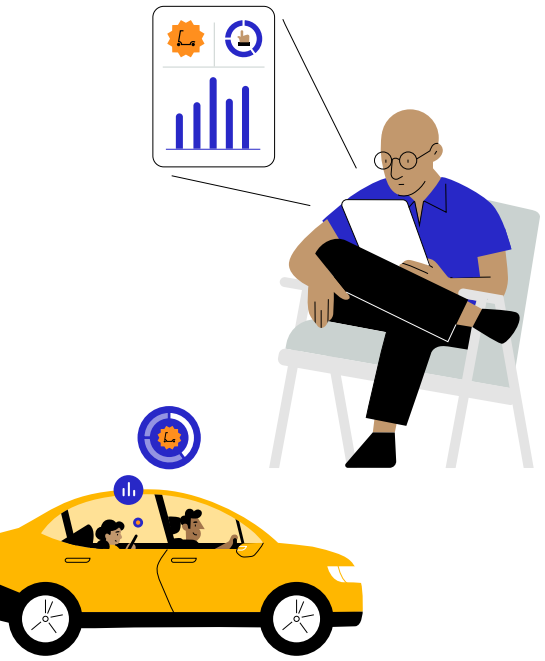
2.
เมื่อ Emma เปิดแอป เครือข่ายโฆษณาก็จะรวบรวมข้อมูลจากการใช้งานบนอุปกรณ์ของ John (เช่น แอปที่เธอกำลังใช้ ตำแหน่งที่ตั้งของเธอ และ ID โฆษณาของ John) รวมถึงข้อมูลจากบริษัทอื่นโดยอาศัย ID โฆษณาของ John หรือข้อมูลอื่นๆ ที่เปิดให้สามารถติดตามได้[3]

3.
เครือข่ายโฆษณาแชร์ข้อมูลเหล่านี้บางส่วน โดยเฉพาะ ID โฆษณา ให้กับใครก็ตามที่มีโอกาสเป็นผู้โฆษณา ซึ่งก่อนเสนอราคา ผู้โฆษณามักพยายามเรียนรู้ข้อมูลเกี่ยวกับผู้ใช้รายนั้นให้มากที่สุดเท่าที่จะเป็นได้ ทั้งจากข้อมูลที่ผู้โฆษณามีอยู่แล้ว และจากข้อมูลส่วนตัวที่เก็บรวบรวมผ่านการติดตามและการทำโปรไฟล์[3,15]

4.
ยิ่งลักษณะเฉพาะของ John และ Emma ที่ได้มาจากข้อมูลของพวกเขาเองสอดคล้องกับกลุ่มเป้าหมายของผู้โฆษณามากเท่าไหร่ ผู้โฆษณาก็จะเสนอราคาสำหรับพื้นที่โฆษณาสูงขึ้นเท่านั้น[15,38]

5
โฆษณารถสกูตเตอร์ของผู้เสนอราคาที่ชนะการประมูลปรากฏบนอุปกรณ์ที่ Emma ใช้งานอยู่[14]

เนื่องจากกระบวนการประมูลโฆษณาเกิดขึ้นในเวลาเพียงเสี้ยววินาที ทั้งผู้ซื้อและผู้ขายจึงคอยเก็บรวบรวม แลกเปลี่ยน และใช้ข้อมูลส่วนตัวเหล่านี้ในการเสนอราคาเพื่อซื้อพื้นที่และแสดงโฆษณา[14,15]



การระบุที่มาของโฆษณา

หลังจากที่โฆษณาของบริษัทถูกแสดงให้ผู้ใช้เห็น บริษัทโฆษณาของบริษัทรถสกูตเตอร์ก็จะให้ความสนใจไปกับการประเมินผล ว่าโฆษณานั้นส่งผลต่อพฤติกรรมของ Emma อย่างไร โดยกระบวนการนี้เรียกว่าการระบุที่มาของโฆษณา

ซึ่งเริ่มจากการที่ผู้โฆษณาพยายามติดตามพฤติกรรมการใช้งานบนอุปกรณ์ที่ Emma ใช้อยู่ เพื่อเก็บข้อมูลเกี่ยวกับสิ่งที่เธอทำบนเว็บ บนแอป หรือแม้แต่สถานที่ที่เธอไปในชีวิตจริง

- **หากเป็นโฆษณาสำหรับผลิตภัณฑ์** ผู้โฆษณาอาจพยายามติดตามว่าหลังจากนั้นผู้ใช้ไปที่เว็บไซต์ของตนหรือไปที่หน้าร้านเพื่อซื้อผลิตภัณฑ์หรือไม่[3]
- **หากเป็นโฆษณาสำหรับแอป** ผู้โฆษณาอาจพยายามติดตามว่าเธอได้ติดตั้งแอปนั้นหรือไม่ ซึ่งกระบวนการนี้เรียกว่าการระบุที่มาของการติดตั้งแอป[39]

นอกจากนี้ผู้โฆษณายังใช้การระบุที่มาของโฆษณาเพื่อ "เพิ่มประสิทธิภาพ" ของแคมเปญโฆษณากับกลุ่มเป้าหมายที่แคมเปญโฆษณานั้นจะได้ผลมากกว่าด้วย[3]

แต่ก็ไม่ใช่ว่าต้องเป็นวิธีนี้เสมอไป เพราะผู้โฆษณาก็สามารถวัดผลของแคมเปญโฆษณาที่เกิดกับกลุ่มเป้าหมายโดยไม่ต้องติดตามผู้ใช้ได้เช่นกัน และตลอดเวลาที่ผ่านมา Apple ก็ได้มุ่งพัฒนาเครื่องมือต่างๆ ที่ทำเช่นนี้ได้ในขณะที่ยังรักษาความเป็นส่วนตัวของผู้ใช้เอาไว้

SKAdNetwork จะคอยแจ้งให้ผู้โฆษณาทราบว่ามีการติดตั้งแอปกี่ครั้งหลังจากที่มีผู้เห็นโฆษณา เพื่อให้ผู้โฆษณาสามารถวัดผลของแคมเปญโฆษณาได้ ซึ่งข้อมูลนี้ถูกออกแบบมาเพื่อไม่ให้มีการแชร์ข้อมูลใดๆ ไม่ว่าจะข้อมูลของผู้ใช้ หรือข้อมูลในระดับอุปกรณ์ต่างๆ ดังนั้นผู้โฆษณาจึงไม่ได้มีการติดตามผู้ใช้

"การวัดผลของการคลิกแบบส่วนตัว" หรือ Private Click Measurement สำหรับแอปใน iOS และ iPadOS 14.5 ช่วยให้ผู้โฆษณาสามารถวัดผลของโฆษณาที่พาผู้ใช้ไปยังเว็บไซต์ และขณะเดียวกันก็ยังลดการเก็บข้อมูลให้น้อยที่สุดโดยใช้การประมวลผลบนอุปกรณ์แทน ซึ่งหลังจากที่ผู้ใช้คลิกโฆษณาสำหรับผลิตภัณฑ์ตัวหนึ่งในแอป "การวัดผลของการคลิกแบบส่วนตัว" จะสามารถให้ข้อมูลกับผู้โฆษณาได้ว่ามีผู้ใช้คลิกโฆษณาของตนและการคลิกนั้นนำไปสู่การกระทำบางอย่างบนเว็บไซต์นั้น เช่น การเข้าไปที่เว็บไซต์หรือการซื้อสินค้า โดยจะไม่มีการให้ข้อมูลที่ระบุอย่างเจาะจงว่าใครเป็นผู้คลิกโฆษณาตัวนี้

คำถามที่พบบ่อย

ถ้าเลือก "บอกแอปไม่ให้ติดตาม" จะยังสามารถใช้แอปได้เต็มความสามารถหรือไม่

แน่นอน นักพัฒนาแอปไม่สามารถบังคับให้คุณต้องอนุญาตการติดตามเพื่อให้ใช้แอปได้เต็มความสามารถ

ตัวบ่งชี้คืออะไรและถูกนำไปใช้อย่างไร

ตัวบ่งชี้ เช่น ตัวบ่งชี้สำหรับผู้โฆษณาหรือ Identifier For Advertisers (IDFA) และที่อยู่อีเมล ช่วยให้สามารถระบุอุปกรณ์ในเครือข่ายได้อย่างเฉพาะเจาะจง และยังช่วยให้ผู้โฆษณาสามารถสร้างโปรไฟล์อย่างละเอียดเกี่ยวกับสิ่งที่คุณทำในแอปหรือเว็บไซต์ต่างๆ เมื่อพวกเขาเห็นตัวบ่งชี้อุปกรณ์ของคุณ และเชื่อมโยงสิ่งที่คุณทำกับตัวบ่งชี้นั้น

ตัวบ่งชี้สำหรับผู้โฆษณาหรือ Identifier For Advertisers (IDFA) คืออะไร

ตัวบ่งชี้สำหรับผู้โฆษณา (IDFA) คือตัวบ่งชี้ที่ผู้ใช้สามารถควบคุมได้ โดย iOS จะเป็นตัวกำหนดให้กับอุปกรณ์แต่ละเครื่อง และเนื่องจากเราใช้ตัวบ่งชี้แบบซอฟต์แวร์ แทนตัวบ่งชี้ที่ผูกอยู่กับฮาร์ดแวร์ ผู้ใช้จึงสามารถบล็อค IDFA สำหรับแอปใดแอปหนึ่งได้ผ่านทางคำแนะนำที่แสดงโดยคุณสมบัติ "ความโปร่งใสในการติดตามของแอป" วิธีนี้จึงช่วยให้ผู้ใช้สามารถควบคุมการติดตามผ่าน IDFA ได้

ถ้าเลือก "บอกแอปไม่ให้ติดตาม" แล้ว Apple จะรับประกันได้หรือไม่ว่าแอปไม่ได้ติดตามฉันอยู่

ถ้าคุณเลือก "บอกแอปไม่ให้ติดตาม" แล้ว นักพัฒนาจะไม่สามารถเข้าใช้งานตัวบ่งชี้สำหรับผู้โฆษณา (IDFA) ซึ่งมักใช้สำหรับการติดตามได้ และนอกเหนือจากข้อมูลโฆษณาประจำตัวแล้ว นักพัฒนาแอปยังต้องเคารพการตัดสินใจของคุณด้วย ซึ่งเป็นสิ่งที่กำหนดไว้ในนโยบายที่นักพัฒนาตกลงยอมรับเมื่อตอนที่ส่งแอปมาเพื่อแจกจ่ายใน App Store และหากเราทราบว่านักพัฒนารายใดยังคงติดตามผู้ใช้ทั้งๆ ที่ผู้ใช้เลือกไม่ให้ติดตามแล้ว เราจะแจ้งให้นักพัฒนาอัปเดตแนวทางปฏิบัติของตนเพื่อเคารพการตัดสินใจของคุณ มิเช่นนั้นแอปดังกล่าวจะถูกนำออกจาก App Store

ถ้าฉันใช้บัญชีโซเชียลมีเดียเพื่อลงชื่อเข้าใช้แอป บริษัทโซเชียลมีเดียจะสามารถติดตามสิ่งที่ฉันทำในแอปนั้นได้หรือไม่

สิ่งนี้ขึ้นอยู่กับว่าคุณได้อนุญาตให้แอปนั้นติดตามคุณหรือไม่ ถ้าคุณเลือก "บอกแอปไม่ให้ติดตาม" แล้ว แอปนั้นก็ไม่ควรติดตามคุณข้ามไปยังแอปหรือเว็บไซต์ของบริษัทอื่นเพื่อการโฆษณา หรือแชร์ข้อมูลของคุณกับนายหน้าหาข้อมูล ซึ่งแปลว่าแอปนั้นไม่ควรให้ข้อมูลของคุณกับบริษัทโซเชียลมีเดีย หากจะมีการนำข้อมูลของคุณไปใช้เพื่อวัตถุประสงค์ดังกล่าว

Apple มั่นใจได้อย่างไรว่าข้อมูลความเป็นส่วนตัวในหน้าผลิตภัณฑ์ของ App Store นั้นถูกต้องตรงความเป็นจริง

นักพัฒนาจะต้องรายงานแนวทางด้านความเป็นส่วนตัวของตนเอง คล้ายกับการกำหนดอายุที่เหมาะกับการใช้งานใน App Store และหากเราทราบว่านักพัฒนารายใดให้ข้อมูลที่ไม่ตรงกับความจริง เราจะติดต่อประสานงานกับนักพัฒนาเพื่อแก้ไขข้อมูลดังกล่าวให้ถูกต้อง

นายหน้าหาข้อมูลหรือ Data Broker คือใคร

โดยทั่วไปแล้ว นายหน้าหาข้อมูลคือบริษัทที่เก็บรวบรวมและจำหน่าย ให้สิทธิ์ใช้งาน หรือเปิดเผยข้อมูลส่วนตัวของผู้ใช้ทั่วไปรายใดรายหนึ่งให้แก่บริษัทอื่นที่ไม่ได้มีความสัมพันธ์ทางธุรกิจโดยตรงกับผู้ใช้รายนั้น และในกฎหมายของบางเขตอำนาจศาลมีการให้คำจำกัดความของนายหน้าหาข้อมูลไว้ด้วย

แหล่งที่มา

1. Gröne, Florian, Pierre Péladeau, et al., "Tomorrow's data heroes" *Strategy+Business,* 19 กุมภาพันธ์ 2020.

2. Reinsel, David, John Gantz, et al., "The Digitization of the World: From Edge to Core," *IDC,* พฤศจิกายน 2018.

3. Competition & Markets Authority, "Online platforms and digital advertising," 1 กรกฎาคม 2020.

4. Hitlin, Paul, and Lee Rainie, "Facebook Algorithms and Personal Data," *Pew Research Center,* 16 มกราคม 2020.

5. AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC," 24 กันยายน 2020.

6. Binns, Reuben, Ulrik Lyngs, et al., "Third Party Track-ing in the Mobile Ecosystem," *Proceedings of the 10th ACM Conference on Web Science,* 2018, หน้า 23-31.

7. MightySignal, "Most Used SDKs in Top 200 Free iOS Apps," mightysignal.com/top-ios-sdks.

8. State of California Department of Justice, "Data Broker Registry," oag.ca.gov/data-brokers.

9. Acxiom Corporation, 2018 Form 10-K, ยื่นเมื่อวันที่ 25 พฤษภาคม 2018, www.sec.gov/Archives/edgar/data/733269/000073326918000016/a2018q410k.htm.

10. Reyes, Irwin, Primal Wijesekera, et al., "'Won't Somebody Think of the Children?' Examining COPPA Compliance at Scale," *Proceedings on Privacy Enhancing Technologies,* ปี 2018, ฉบับที่ 3, 2018, หน้า 63-83.

11. Edwards, Jim, "Here's The Staggering Number of Ads Facebook Serves On Its Exchange Every Day," *Business Insider,* 9 พฤศจิกายน 2012.

12. Kim, Larry, "How Many Ads Does Google Serve In A Day?," *Business 2 Community,* 2 พฤศจิกายน 2012.

13. Deighton, John, and Leora Kornfeld, "The Socioeco-nomic Impact of Internet Tracking," *Interactive Advertising Bureau,* กุมภาพันธ์ 2020.

14. Hwang, Tim, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet,* FSG Originals, 13 ตุลาคม 2020.

15. Australian Competition and Consumer Commission, "Digital advertising services inquiry - Interim report," ธันวาคม 2020.

16. Thompson, Stuart A., and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *The New York Times*, 19 ธันวาคม 2019.

17. Nanos, Janelle, "Every step you take: How companies use geolocation data to target you – and everyone around – in ways you're not even aware of," *The Boston Globe*, 21 กรกฎาคม 2018.

18. Vitaldevara, Krish, "Safer and More Transparent Access to User Location," *Android Developers Blog*, 19 กุมภาพันธ์ 2020.

19. Schechner, Sam, and Mark Secada, "You Give Apps Sensitive Personal Information. Then They Tell Facebook," *The Wall Street Journal*, 22 กุมภาพันธ์ 2019.

20. Facebook for Business, "Measuring Conversions on Facebook, Across Devices and in Mobile Apps," 14 สิงหาคม 2014.

21. Bender, Brad, "New digital innovations to close the loop for advertisers," *Google Ads & Commerce Blog*, 26 กันยายน 2016.

22. Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Face-book," 24 กรกฎาคม 2019.

23. Chin, Kimberly, "Twitter Could Pay FTC Fine Over Alleged Privacy Violations," *The Wall Street Journal*, 3 สิงหาคม 2020.

24. Satariano, Adam, "Google Is Fined $57 Million Under Europe's Data Privacy Law," *The New York Times*, 21 มกราคม 2019.

25. Schiffer, Zoe, "Period tracking app settles charges it lied to users about privacy," *The Verge*, 13 มกราคม 2021.

26. Thompson, Stuart A., "These Ads Think They Know You," *The New York Times*, 30 เมษายน 2019.

27. Venkatadri, Giridhari, Piotr Sapiezynski, et al., "Auditing Offline Data Brokers via Facebook's Advertising Platform," *The World Wide Web Conference*, 2019, หน้า 1920-1930.

28. Leetaru, Kalev, "The Data Brokers So Powerful Even Facebook Bought Their Data - But They Got Me Wildly Wrong," *Forbes*, 5 เมษายน 2018.

29. Grothaus, Michael, "The top 7 iOS 14 privacy features: What you need to know," *Fast Company*, 16 กันยายน 2020.

30. Germain, Thomas, "How a Photo's Hidden 'Exif' Data Exposes Your Personal Information," *Consumer Reports*, 6 ธันวาคม 2019.

31. Helm, Burt, "Credit card companies are tracking shop-pers like never before: Inside the next phase of surveillance capitalism," *Fast Company*, 12 พฤษภาคม 2020.

32. Ramirez, Edith, Julie Brill, et al., "Data Brokers: A Call for Transparency and Accountability," *Federal Trade Commission*, พฤษภาคม 2014.

33. Oracle, "12 Must-Ask Questions to Separate Fact from Fiction," www.oracle.com/a/ocom/docs/idg-12-must-ask-questions-for-identity-vendors.pdf.

34. Hern, Alex, "'Anonymous' browsing data can be easily exposed, researchers reveal," *The Guardian*, 1 สิงหาคม 2017.

35. Fowler, Geoffrey A., "You watch TV. Your TV watches back," *The Washington Post*, 18 กันยายน 2019.

36. X-Mode, "Data Licensing," xmode.io/data-licensing/.

37. หากอายุของผู้ใช้ที่เชื่อมโยงกับ Apple ID ที่ลงทะเบียนกับอุปกรณ์ต่ำกว่า 18 ปี การเข้าถึง IDFA จะถูกกำหนดให้ปิดไว้ตามค่าเริ่มต้น และไม่สามารถอนุญาตให้นักพัฒนารายใดเข้าถึงได้

38. Google Ads Help, "About Smart Bidding," support.google.com/google-ads/answer/7065882?hl=en.

39. Litfin, Marne, "What is Mobile ad attribution? An introduction to app tracking," *Adjust*, 4 กุมภาพันธ์ 2019.

40. Cox, Joseph, "The IRS Is Being Investigated for Using Location Data Without a Warrant," *Vice*, 6 ตุลาคม 2020.

41. Cox, Joseph, "How the U.S. Military Buys Location Data from Ordinary Apps," *Vice*, 16 พฤศจิกายน 2020.

42. Cox, Joseph, "CBP Bought 'Global' Location Data from Weather and Game Apps," *Vice*, 6 ตุลาคม 2020.