

## คำแปลอย่างไม่เป็นทางการ

### จดหมายเปิดผนึกองค์กรสิทธิมนุษยชนทั่วโลก

#### เรียกร้องให้ยุติการใช้เทคโนโลยีชีวมิติซึ่งนำไปสู่การสอดแนมประชาชน

#### ฉบับภาษาอังกฤษ

ในนามของบุคคลและองค์กรที่ได้ลงชื่อไว้ในท้ายจดหมายขอเรียกร้องให้ยุติการใช้ระบบการจดจำใบหน้า (Facial Recognition) และ การใช้เทคโนโลยีชีวมิติระยะไกล (Remote Biometric Recognition Technologies) ซึ่งนำไปสู่การสอดแนมประชาชน (Mass Surveillance) และการสอดแนมประชาชนอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง (Discriminatory Surveillance)

ระบบการจดจำใบหน้าและการใช้เทคโนโลยีชีวมิติระยะไกลคือเครื่องมือที่มีความสามารถในการระบุ ตัวตนติดตาม มุ่งเป้าเฉพาะไปที่ตัวบุคคล และติดตามตัวไปได้ทุกที่ที่กลุ่มเป้าหมายไป ซึ่งการกระทำเหล่านี้เป็นการบ่อนทำลายสิทธิมนุษยชนและเสรีภาพของประชาชนรวมถึงสิทธิส่วนบุคคล การคุ้มครองข้อมูลส่วนบุคคล สิทธิและเสรีภาพในการแสดงความคิดเห็น สิทธิในการชุมนุมอย่างสันติ (ซึ่งทำให้การชุมนุมเป็นอาชญากรรม และทำให้เกิดความหวาดกลัวต่อการใช้สิทธิตามหลักสากล) และสิทธิในความเท่าเทียมและการไม่เลือกปฏิบัติ

เราได้ตระหนักถึงการใช้ระบบการจดจำใบหน้าและการใช้เทคโนโลยีชีวมิติระยะไกล ในฐานะเครื่องมือที่มีความสามารถในการระบุตัวตนที่นำไปสู่การละเมิดสิทธิมนุษยชน ในประเทศจีน สหรัฐอเมริกา รัสเซีย อังกฤษ อูกันดา เคนยา สโลวีเนีย เมียนมาร์ สหรัฐอาหรับเอมิเรตส์ อิสราเอล และอินเดีย การสอดแนมผู้ชุมนุมและประชาชนนำไปสู่การละเมิดสิทธิส่วนบุคคลและสิทธิในการชุมนุมสาธารณะ การจับกุมผู้บริสุทธิ์โดยมิชอบในสหรัฐอเมริกา อาร์เจนตินา และบราซิลเป็นการบ่อนทำลายสิทธิส่วนบุคคลและสิทธิต่างๆที่เกี่ยวกับเสรีภาพในการเคลื่อนไหวทางการเมือง อีกทั้งยังมีการสอดแนมประชาชนในกลุ่มชาติพันธุ์และชนกลุ่มน้อยทางศาสนา รวมไปถึงกลุ่มคนชายขอบที่ถูกกีดกันทางสังคมและกลุ่มคนที่ถูกกดขี่ในประเทศจีน ไทย และอิตาลี ที่มีการละเมิดสิทธิส่วนบุคคล สิทธิในความเท่าเทียม และสิทธิในการไม่ถูกเลือกปฏิบัติของกลุ่มคนเหล่านี้

เทคโนโลยีดังกล่าวถูกออกแบบให้เป็นภัยต่อสิทธิขั้นพื้นฐานของประชาชน อีกทั้งยังทำให้เกิดอันตราย ทั้งนี้ยังไม่มีมาตรการป้องกันข้อมูลส่วนบุคคลทางเทคโนโลยีและกฎหมายที่สามารถลบล้างภัยคุกคามที่เกิดขึ้นได้ ดังนั้นเราจึงไม่สามารถมั่นใจได้ว่าเทคโนโลยีดังกล่าวควรที่จะนำมาใช้กับสาธารณะหรือที่สามารถเข้าถึงได้โดยสาธารณะไม่ว่าจะเป็นจากภาครัฐหรือเอกชน เทคโนโลยีเหล่านี้สามารถนำไปใช้ในทางที่ผิดและมีโอกาสที่จะนำไปสู่การละเมิดสิทธิขั้นพื้นฐานหรือไม่ อีกทั้งผลกระทบที่ตามมาที่ร้ายแรงมากด้วย

เราจึงขอเรียกร้องให้ยุติการใช้เทคโนโลยีดังกล่าว การหยุดใช้ชั่วคราวจะชะลอการพัฒนาและการใช้เทคโนโลยีไปได้บ้าง และเพื่อให้เวลาทบทวนแนวทางตามรูปแบบประชาธิปไตยก่อนการเก็บข้อมูลดังกล่าวต่อไป แต่ก็เป็นที่ประจักษ์แล้วว่า การใช้เทคโนโลยีเหล่านี้ในที่ที่สามารถเข้าถึงโดยสาธารณะมีความขัดแย้งกับหลักการสิทธิมนุษยชนและเสรีภาพของประชาชน ซึ่งการกระทำดังกล่าวต้องยุติโดยทันที

#### ขอบเขตข้อเรียกร้องจากเรา

ความหมายของคำว่า “การจดจำใบหน้า (Facial Recognition)” และ “การจดจำข้อมูลชีวมิติระยะไกล (Remote Biometric Recognition)” ครอบคลุมเทคโนโลยีด้านนี้อย่างกว้างขวางตั้งแต่ระบบการยืนยันตัวตนโดยใช้ใบหน้าที่ใช้ในการปลดล็อกโทรศัพท์มือถือ หรือการอนุญาตการเข้าถึงของบุคคลในพื้นที่ต่างๆ รวมทั้งเทคโนโลยีที่สามารถระบุท่าทางการเดิน และระบบที่สามารถระบุเพศสภาพหรือการแสดงอารมณ์ของผู้ใช้งาน

ข้อเรียกร้องของเราให้ความสำคัญเรื่องการยุติการใช้เทคโนโลยีดังกล่าวในการระบุตัวตนหรือคัดแยกตัวบุคคลจากกลุ่มคน ซึ่งเป็นที่รู้จักในนาม “การยืนยันตัวบุคคลด้วยใบหน้า (Facial Identification)” หรือ “การยืนยันตัวบุคคลโดยข้อมูลชีวภาพ (Biometric Identification)” (เช่น ฐานข้อมูลแบบหนึ่งต่อกลุ่ม หรือ One-to-many Matching) อย่างไรก็ตามข้อเรียกร้องของเราไม่ได้จำกัดแต่เพียงเท่านั้น เรามีความกังวลต่อการใช้เทคโนโลยีดังกล่าวในการระบุตัวตน มุ่งเป้าเฉพาะไปที่ตัวบุคคล หรือการติดตามตัวบุคคลจากการใช้การระบุใบหน้า ท่าทางการเดิน เสียง รูปร่าง

ลักษณะเฉพาะตัว หรือข้อมูลทางชีวมิติอื่นๆ ซึ่งสามารถทำให้เกิดการสอดแนมประชาชน หรือการสอดแนมประชาชนอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง เช่น การสอดแนมที่ส่งผลต่อการละเมิดสิทธิมนุษยชนและเสรีภาพของประชาชนในด้านของศาสนา ชาติพันธุ์ หรือชนกลุ่มน้อย ผู้เห็นต่างทางการเมือง หรือกลุ่มคนที่ถูกกีดกันทางสังคม อีกทั้งเรายังได้ทราบว่าในบางกรณี การใช้ระบบการยืนยันตัวบุคคลด้วยใบหน้า หรือการยืนยันตัวบุคคลโดยชีวภาพ (เช่น ฐานข้อมูลแบบหนึ่งต่อหนึ่ง) สามารถก่อให้เกิดปัญหาการสอดแนมได้เช่นกัน เช่น การสร้างฐานข้อมูลชีวมิติขนาดใหญ่และรวมศูนย์กลาง ทำให้เกิดการนำข้อมูลไปใช้ซ้ำซ้อนกับระบบอื่น

ถึงแม้ว่าบางแอปพลิเคชันที่มีการใช้ระบบการจดจำใบหน้าหรือระบบการจดจำชีวมิติระยะไกลได้อ้างถึงความสามารถในการปกป้องข้อมูลส่วนบุคคลโดยกล่าวว่าข้อมูลที่จะไม่มีการเชื่อมโยงและไม่มีความเกี่ยวข้องกับความเป็นบุคคลทางกฎหมาย (Legal Identities) อย่างไรก็ตาม ข้อมูลดังกล่าวก็สามารถใช้ในการระบุตัวบุคคลโดยเฉพาะเจาะจงจากพื้นที่สาธารณะ หรือสามารถเข้าไปแทรกแซงลักษณะส่วนบุคคลและพฤติกรรมต่างๆ จากสถานการณ์ดังกล่าว การทำให้ข้อมูลทางชีวมิติไม่สามารถระบุตัวตนเพื่อเป็นการป้องกันข้อมูลที่สามารถใช้ในการระบุตัวตนนั้นไม่เพียงพอ สิ่งสำคัญคือข้อมูลเหล่านี้ยังสามารถนำไปสู่การละเมิดสิทธิในด้านต่างๆ เนื่องจากเครื่องมือเหล่านี้ถูกออกแบบมาเพื่อการสอดแนมประชาชน ซึ่งการกระทำดังกล่าวถือเป็นการขัดต่อสิทธิของเรา

ยิ่งไปกว่านั้น แอปพลิเคชันต่างๆที่ใช้เพื่อการแบ่งแยกใบหน้าและข้อมูลชีวมิติซึ่งก่อให้เกิดการอ้างอิงและการคาดเดาข้อมูลต่างๆจากเพศสภาพของผู้ใช้ อารมณ์ หรือลักษณะส่วนตัวอื่นๆ ซึ่งมีข้อบกพร่องทางฐานข้อมูลทางวิทยาศาสตร์ ข้อมูลเหล่านี้ชี้ให้เห็นว่าการคาดเดาเกี่ยวกับตัวตนของเราจากแอปพลิเคชันต่างๆเกิดข้อผิดพลาดอยู่บ่อยครั้ง โดยเฉพาะในบางกรณีได้มีการใช้ทฤษฎีพันธุศาสตร์ในด้านของการคาดเดานิยายจากกระโหลกศีรษะและใบหน้า ดังนั้นการใช้แอปพลิเคชันดังกล่าวจึงเป็นการส่งเสริมการเลือกปฏิบัติและเพิ่มความซับซ้อนของความปลอดภัยที่เกิดจากการสอดแนมและการระบุตัวตนที่ผิดพลาด

ข้อเรียกร้องของเราครอบคลุมถึงการใช้งานของเทคโนโลยีดังกล่าวเมื่อถูกใช้เพื่อสอดแนมในที่สาธารณะหรือในพื้นที่ที่ไม่สามารถหลีกเลี่ยงการใช้งานได้ (พื้นที่ที่เราจำเป็นต้องไปอย่างหลีกเลี่ยงไม่ได้) ในขณะที่การบังคับใช้กฎหมายที่เกี่ยวข้องยังอยู่ในความสนใจและถูกวิพากษ์วิจารณ์ ภาคเอกชนก็ได้มีการใช้เทคโนโลยีเหล่านี้เช่นกัน ถึงกระนั้นการใช้งานเทคโนโลยีดังกล่าวจากภาคเอกชนก็สามารถเป็นภัยต่อสิทธิของเราเช่นกัน โดยเฉพาะอย่างยิ่งเมื่อภาคเอกชนสามารถสอดแนมให้รัฐบาลหรือหน่วยงานรัฐในนามของความร่วมมือระหว่างภาครัฐและเอกชน (Public-Private Partnership) หรือแม้กระทั่งการจัดการจัดหาข้อมูลต่างๆที่ได้จากการสอดแนมได้

เราได้ตระหนักถึงการที่ระบบการจดจำใบหน้าของภาคเอกชนที่กำลังเติบโตในฐานของผู้ให้ข้อมูลและเป็นที่รวบรวมข้อมูลของบุคคลต้องสงสัย รวมถึงยังได้มีการแบ่งปันฐานข้อมูลร่วมกับลูกค้าหลายกลุ่ม การกระทำดังกล่าวทำให้เกิดฐานข้อมูลที่ใช้ร่วมกันทั่วประเทศ ซึ่งเป็นการใช้ฐานข้อมูลร่วมกันระหว่างบริษัทเอกชนดูแลโดยกลุ่มพนักงานที่ไม่ได้รับการฝึกฝน อีกทั้งยังไม่มีกระบวนการควบคุมดูแล ซึ่งสามารถนำไปสู่การเลือกปฏิบัติต่อผู้ที่อยู่ในบัญชีการเฝ้าระวังของฐานข้อมูล

การใช้เทคโนโลยีดังกล่าวในการสอดแนมผู้คนในสวนสาธารณะ โรงเรียน ห้องสมุด ที่ทำงาน ศูนย์กลางในการขนส่ง สนามกีฬา ที่อยู่อาศัย และรวมไปถึงพื้นที่ออนไลน์ เช่น โซเชียลมีเดีย ซึ่งเป็นภัยต่อสิทธิมนุษยชนและเสรีภาพของพลเมืองซึ่งการกระทำเหล่านี้ต้องยุติลง

## เหตุใดจึงต้องยุติการใช้เทคโนโลยีเหล่านี้

เทคโนโลยีระบบการจดจำใบหน้าและระบบการจดจำชีวมิติในรูปแบบปัจจุบันมีข้อผิดพลาดทางเทคนิคอย่างมีนัยยะสำคัญ ตัวอย่างเช่นระบบการจดจำใบหน้าได้สะท้อนถึงอคติทางเชื้อชาติต่อคนที่มีสีผิวเข้ม อย่างไรก็ตามการแก้ไขข้อผิดพลาดของระบบตรงจุดนี้ก็ไม่สามารถลบล้างภัยที่มีต่อสิทธิมนุษยชนและเสรีภาพของพลเมือง

การปรับปรุงระบบหรือเพิ่มเติมข้อมูลต่างๆเพื่อพัฒนาความถูกต้องของเทคโนโลยีนี้เป็นการเพิ่มประสิทธิภาพของการสอดแนมและบ่อนทำลายสิทธิของเราในด้านต่างๆ

เทคโนโลยีดังกล่าวก่อให้เกิดภัยต่อสิทธิของเราในสองด้านหลัก ดังต่อไปนี้:

หนึ่ง ข้อมูลที่ใช้เพื่อทดสอบคอมพิวเตอร์ (Training Data) คือฐานข้อมูลที่ถูกป้อนเข้าระบบโดยเปรียบเทียบในการใช้เป็นแม่พิมพ์ของระบบข้อมูลชีวมิติ โดยข้อมูลเหล่านี้มักได้มาโดยไม่ได้รับความยินยอม ซึ่งกล่าวได้ว่าถึงเทคโนโลยีดังกล่าวถูกออกแบบให้สนับสนุนการสอดแนมประชาชน

สอง トラブิตที่ผู้คนอยู่ในพื้นที่ที่เข้าถึงได้โดยสาธารณะ พวกเขาจะสามารถถูกระบุตัวตน มุ่งเป้าเฉพาะ หรือถูกติดตามได้โดยทันที ซึ่งเป็นการละเมิดสิทธิมนุษยชนและเสรีภาพประชาชน ทั้งนี้เทคโนโลยีดังกล่าวยังทำให้เกิดความหวาดกลัวซึ่งทำให้ผู้คนไม่กล้าที่จะใช้สิทธิและเสียงของตัวเอง ถึงแม้ว่าเทคโนโลยีดังกล่าวจะทำให้เกิดการพัฒนาคความปลอดภัยในสาธารณะแต่การละเมิดสิทธิที่เกิดจากการใช้งานของเทคโนโลยีนี้เป็นสิ่งที่ต้องให้ความสำคัญมากกว่า ดังจะเห็นได้จากข้อมูลและหลักฐานของการใช้เทคโนโลยีดังกล่าวในทางที่ผิด และยังขาดความโปร่งใส

งานสำรวจต่างๆได้พบว่าหน่วยงานตำรวจได้ทดลองใช้งานเทคโนโลยีการสอดแนมกับกลุ่มผู้มียาได้น้อยและกลุ่มคนชายขอบ รวมทั้งกลุ่มคนตาซึ่งเป็นผู้ที่ถูกกดทับจากการเหยียดเชื้อชาติและการถูกเลือกปฏิบัติ การใช้งานของระบบการจดจำใบหน้าและการจดจำชีวมิติระยะไกลไม่สามารถเป็นที่ยอมรับได้ และควรได้รับการยุติก่อนที่จะถูกพัฒนาให้เป็นเครื่องมือติดตามโดยถาวร

การมีอยู่ของเทคโนโลยีเหล่านี้ทำให้เกิดแรงจูงใจในการสอดแนมในพื้นที่สาธารณะ ไม่ว่าจะเป็นการใช้งานโดยภาครัฐหรือเอกชน การใช้งานของเทคโนโลยีเหล่านี้ทำให้เกิดความหวาดกลัวในการใช้สิทธิในการแสดงความคิดเห็น เนื่องจากการมีอยู่ของเทคโนโลยีดังกล่าวได้บั่นทอนสิทธิของเรา อีกทั้งยังขาดการควบคุมการใช้งานที่สามารถยับยั้งการละเมิดสิทธิได้ ดังนั้นการยุติการใช้งานเทคโนโลยีเหล่านี้ทั้งหมดในพื้นที่สาธารณะจึงเป็นทางเลือกเดียวที่ทุกฝ่ายต้องทำ

## การยุติจะเกิดขึ้นได้อย่างไร?

เทคโนโลยีการสอดส่องจำนวนหนึ่งมีความอันตรายอย่างมากซึ่งเป็นสิ่งที่นำมาสู่ปัญหามากกว่าการแก้ไขอย่างหลีกเลี่ยงไม่ได้ ระบบการจดจำใบหน้า และการใช้เทคโนโลยีชีวมิติระยะไกล สามารถใช้ในการสอดแนมประชาชนและการสอดแนมอย่างเลือกปฏิบัติที่มุ่งเป้าเฉพาะประชาชนบางกลุ่มได้ โดยเทคโนโลยีเหล่านี้มีความเสี่ยงอย่างมากที่จะถูกใช้ในทางที่ผิด และนำมาสู่ผลลัพธ์ที่ร้ายแรง

ฉะนั้นจึงปฏิเสธไม่ได้เลยว่า การคุ้มครองสิทธิมนุษยชนและเสรีภาพของประชาชนนั้นจำเป็นต้องมีการยุติการใช้เทคโนโลยีดังกล่าวในพื้นที่สาธารณะ จากรัฐบาลทุกระดับตั้งแต่ระดับชาติไปจนถึงระดับท้องถิ่น และโดยเฉพาะอย่างยิ่งในส่วนของผู้บังคับใช้กฎหมายและหน่วยงานที่ควบคุมบริเวณพื้นที่ชายแดน ซึ่งเป็นหน่วยงานที่มีทั้งทรัพยากรมนุษย์และเทคโนโลยีมาเพียงพอแล้วในการรักษาความปลอดภัย

ในนามเครือข่ายองค์กรภาคประชาสังคมระดับโลก เราตระหนักดีว่าทุกประเทศมีวิธีการในการแก้ไขปัญหาที่ให้ความสำคัญกับสิทธิมนุษยชนแตกต่างกันออกไปตามรัฐธรรมนูญ ธรรมเนียมปฏิบัติ และระบบกฎหมายของแต่ละประเทศ

แต่ไม่ว่าวิธีการจะเป็นอย่างไร ผลลัพธ์ที่ได้ต้องเป็นการยุติการใช้เทคโนโลยีดังกล่าวในการสอดแนม, ระบุตัวตน, สะกดรอย, แบ่งแยก และติดตามประชาชนในพื้นที่สาธารณะ

ด้วยเหตุผลที่กล่าวไปข้างต้น พวกเราเรียกร้องให้ผู้มีส่วนเกี่ยวข้องปฏิบัติตามข้อเสนอ ดังต่อไปนี้

1. ผู้กำหนดนโยบาย และผู้ออกกฎหมายทุกระดับในหน่วยงานของรัฐ ทุกประเทศ
  - a. ยุติการลงทุนของภาครัฐในระบบการจดจำใบหน้าและเทคโนโลยีชีวมิติระยะไกลที่สามารถใช้ในการสอดแนมประชาชน การสอดแนมประชาชนอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง
  - b. บังคับใช้กฎหมาย, พระราชบัญญัติ และ/หรือ ข้อบังคับ ที่:
    - i. ยับยั้งการใช้เทคโนโลยีดังกล่าวเพื่อการสอดแนมประชาชนทั้งในพื้นที่สาธารณะและพื้นที่ที่สามารถเข้าถึงได้อย่างสาธารณะ ซึ่งรวมถึง ระบบขนส่งสาธารณะที่จัดตั้งโดยรัฐหรือในนามของรัฐบาลระดับชาติ, ท้องถิ่น และ/หรือ หน่วยงานของ

เขตการปกครองของรัฐ โดยเฉพาะอย่างยิ่งในส่วนของกำบังคับใช้กฎหมาย, การสืบสวนอาชญากรรม, การควบคุมบริเวณพื้นที่ชายแดน และหน่วยข่าวกรอง

ii. ยับยั้งการใช้เทคโนโลยีดังกล่าวโดยหน่วยงานเอกชนในพื้นที่สาธารณะ, พื้นที่ที่สามารถเข้าถึงได้อย่างสาธารณะ และพื้นที่ที่รัฐหรือเอกชนเป็นเจ้าของและประชาชนสามารถเข้าถึงได้ ซึ่งสามารถมีการสอดแนมประชาชนและสอดแนมอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่งได้ ซึ่งรวมถึงแต่ไม่จำกัดเพียงการใช้ในสวนสาธารณะ, โรงเรียน, ห้องสมุด, ที่ทำงาน, จุดขนส่ง, สนามกีฬาและที่อยู่อาศัย

iii. ยับยั้งหน่วยงานรัฐโดยเฉพาะผู้บังคับใช้กฎหมายจากการเข้าถึงและใช้ประโยชน์จากข้อมูลที่มาจากเทคโนโลยีดังกล่าวของบริษัทเอกชนและหน่วยงานอื่นๆที่ไม่ใช่รัฐ ยกเว้นเป็นไปเพื่อการตรวจสอบบัญชี หรือการตรวจสอบการปฏิบัติตามข้อกำหนดขององค์กร

iv. คัดกรองประชาชนจากการใช้เทคโนโลยีดังกล่าวในการตัดสินใจที่เกี่ยวข้องกับสิทธิทางเศรษฐกิจ, สังคม และวัฒนธรรม รวมไปถึงในประเด็นที่อยู่อาศัย, การจ้างงาน, สวัสดิการสังคม และการบริการสุขภาพ

v. ยกเว้นการใช้เทคโนโลยีดังกล่าวและข้อมูลที่ได้รับ เป็นหลักฐานในการดำเนินคดีอาญาหรือกล่าวหาบุคคลอื่นให้ถูกกักขังหรือจำคุก

vi. จำกัดการเข้าถึงข้อมูลชีวมิติโดยรัฐที่จัดเก็บโดยบริษัทเอกชน

c. จัดตั้งระเบียบและข้อบังคับที่ห้ามไม่ให้มีการจัดซื้อเทคโนโลยีดังกล่าวโดยรัฐและหน่วยงานของรัฐในการใช้เพื่อสอดแนมประชาชน การสอดแนมอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง

d. ยุติการใช้ระบบการจดจำใบหน้าและเทคโนโลยีชีวมิติระยะไกลเพื่อสอดแนมประชาชนหรือการสอดแนมอย่างเลือกปฏิบัติที่เจาะจงไปที่ชนกลุ่มน้อยทางศาสนา, ชาติพันธุ์ และเชื้อชาติ รวมไปถึงผู้เห็นต่างทางการเมืองและกลุ่มคนชายขอบอื่นๆ

e. บังคับให้มีการเปิดเผยการใช้เทคโนโลยีดังกล่าวต่อบุคคลที่ถูกใช้เทคโนโลยีโดยไม่รู้ตัวและไม่มีโอกาสได้ใช้สิทธิในการโต้แย้งการใช้เทคโนโลยีดังกล่าว

f. จัดหาการชดเชยที่เหมาะสมให้กับผู้เสียหายที่ได้รับผลกระทบจากการใช้เทคโนโลยีดังกล่าว

2. ศาลและเจ้าหน้าที่ตุลาการ ควรรับรู้ถึงภัยคุกคามต่อสิทธิมนุษยชนอันเกิดขึ้นจากการใช้เทคโนโลยีดังกล่าว และควรดำเนินการป้องกันพร้อมทั้งหาทางแก้ไขเพื่อชดเชยความเสียหายที่เกิดขึ้นหากจำเป็น

3. หน่วยงานบริหาร อันรวมถึงหน่วยงานคุ้มครองข้อมูล และหน่วยงานคุ้มครองผู้บริโภคควรรื้อฟื้นอย่างเต็มที่ในการคุ้มครองความเป็นส่วนตัวและสิทธิผู้บริโภค รวมไปถึงเรียกร้องให้บริษัทต่างๆยุติการใช้เทคโนโลยีดังกล่าว

สุดท้ายนี้ เราตระหนักดีว่าภัยคุกคามจากระบบการจดจำใบหน้าและเทคโนโลยีชีวมิติระยะไกลไม่ใช่หน้าที่ของประเทศและรัฐบาลในการจัดการเท่านั้น แต่ยังเป็นหน้าที่ของตัวแสดงอื่นๆ ทั้งในระดับนานาชาติ และระดับประเทศที่จะยุติปัญหานี้

### ด้วยเหตุผลดังกล่าว เราจึงเรียกร้องให้ :

1. องค์การระหว่างประเทศ เช่น สำนักงานข้าหลวงใหญ่สิทธิมนุษยชนแห่งสหประชาชาติ (The Office of the United Nations High Commissioner for Human Rights - OHCHR) เข้ามามีบทบาทและประสานการพัฒนากระบวนการจดจำใบหน้าและเทคโนโลยีชีวมิติระยะไกลที่จัดทำขึ้นเพื่อสอดแนมประชาชนในรัฐต่างๆทั่วโลก

2. หน่วยงานเอกชน ที่พัฒนาหรือใช้ระบบการจดจำใบหน้าและเทคโนโลยีชีวมิติระยะไกล :
  - a. ให้คำมั่นสัญญาต่อสาธารณะว่าจะยุติการสร้าง พัฒนา รวมถึงจำหน่าย ระบบการจดจำใบหน้าและเทคโนโลยีชีวมิติระยะไกลที่สามารถใช้ในการสอดแนมประชาชนและการสอดแนมอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง
  - b. ยุติการผลิตระบบการจดจำใบหน้าและเทคโนโลยีชีวมิติระยะไกลที่ใช้ในการสอดแนมประชาชนและการสอดแนมอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง รวมทั้งลบข้อมูลชีวมิติที่ได้มาโดยมิชอบด้วยกฎหมายที่ใช้ในการสร้างฐานข้อมูลและต้นแบบ หรือผลิตภัณฑ์ใดๆก็ตามที่สร้างขึ้นจากข้อมูลดังกล่าว
  - c. เผยแพร่รายงานความโปร่งใสที่ระบุถึงรายละเอียดของสัญญาที่ทำกับภาครัฐทั้งหมด (รวมถึงสัญญาที่ถูกระงับ, อยู่ระหว่างการดำเนินการ หรือกำลังจัดทำ) สำหรับการจัดการเทคโนโลยีดังกล่าว
  - d. มีส่วนร่วมและไม่ทำการต่อต้านกลุ่มพนักงานที่ทำหายหรือปฏิเสธการพัฒนาหรือจำหน่ายระบบการจดจำใบหน้าและเทคโนโลยีชีวมิติระยะไกลที่ใช้ในการสอดแนมประชาชนและการสอดแนมอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง
3. พนักงานของบริษัทเทคโนโลยี : พร้อมทั้งการสนับสนุนจากสหภาพแรงงาน ควรทำการต่อต้านการพัฒนาหรือจำหน่ายระบบการจดจำใบหน้าและเทคโนโลยีชีวมิติระยะไกลเท่าที่สามารถกระทำได้
4. นักลงทุน และสถาบันการเงิน :
  - a. ดำเนินการตรวจสอบประเด็นสิทธิมนุษยชนกับบริษัทที่พัฒนาและจำหน่ายระบบการจดจำใบหน้าและเทคโนโลยีชีวมิติระยะไกลที่ได้ทำการลงทุนไปในปัจจุบันและที่จะลงทุนในอนาคตเพื่อตรวจสอบว่ามีส่วนใดของเทคโนโลยีหรือไม่ ที่ไม่สอดคล้องกับหลักสิทธิมนุษยชนและสามารถใช้ในการสอดแนมประชาชนและการสอดแนมอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง
  - b. เรียกร้องให้บริษัทได้ลงทุนไป ยุติการสร้าง พัฒนา จำหน่าย หรือทำให้เทคโนโลยีดังกล่าวไปสามารถใช้งานได้ ในลักษณะที่สามารถใช้ในการสอดแนมประชาชนและการสอดแนมอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง
5. องค์กรผู้บริจาค ควรตรวจสอบให้แน่ใจว่ามีเงินทุนสำหรับการดำเนินคดีความและการรณรงค์ให้กับองค์กรที่ไม่ใช่รัฐและองค์กรภาคประชาสังคมที่แสวงหาทางแก้ปัญหาทั้งในชั้นศาลและมีส่วนร่วมอย่างจริงจังในการกำหนดนโยบายทั้งในระดับรัฐบาลท้องถิ่น ระดับชาติ รวมทั้งในระดับเหนือชาติ ระดับภูมิภาค และในระบาระหว่างประเทศ

## สรุป

เราเรียกร้องให้ภาคประชาสังคม, นักกิจกรรม, นักวิชาการ, และผู้ที่เกี่ยวข้อง ทั่วโลกร่วมลงชื่อในจดหมายนี้และร่วมกันต่อสู้เพื่อให้มีการยุติการใช้เทคโนโลยีดังกล่าวในพื้นที่ที่เข้าถึงได้อย่างสาธารณะโดยถาวรเพื่อปกป้องและคุ้มครองสิทธิมนุษยชนและเสรีภาพของมนุษย์

---

จดหมายเปิดผนึกนี้จัดทำขึ้นโดย Access Now, Amnesty International, European Digital Rights (EDRI), Human Rights Watch, Internet Freedom Foundation (IFF), and Instituto Brasileiro de Defesa do Consumidor (IDEC) และลงนามโดยองค์กรทั่วโลกจำนวน 179 องค์กร

แปลเป็นภาษาไทยอย่างไม่เป็นทางการโดย มูลนิธิผสานวัฒนธรรม (Cross Cultural Foundation)

โดย ธวัชรัตน์ ม้าฤทธิ์ และ นัทธมน ศุภรเวทย์

## คำแปลศัพท์เฉพาะอย่างไม่เป็นทางการในจดหมายนี้

1. ระบบการจดจำใบหน้า (Facial Recognition)
2. การใช้เทคโนโลยีชีวมิติระยะไกล (Remote Biometric Recognition Technologies)
3. การสอดแนมประชาชน (Mass Surveillance)
4. การสอดแนมประชาชนอย่างเลือกปฏิบัติในกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง (Discriminatory Surveillance)
5. การจดจำใบหน้า (Facial Recognition)
6. การจดจำข้อมูลชีวมิติระยะไกล (Remote Biometric Recognition)
7. การยืนยันตัวตนบุคคลด้วยใบหน้า (Facial Identification)
8. การยืนยันตัวตนบุคคลโดยข้อมูลชีวภาพ (Biometric Identification)
9. ฐานข้อมูลแบบหนึ่งต่อกลุ่ม (One-to-many Matching)
10. ความเป็นบุคคลทางกฎหมาย (Legal Identities)

[accessnow.org/ban-biometric-surveillance](https://accessnow.org/ban-biometric-surveillance)