LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

RAND CORPORATION

هل يمكن للخصوصية والهاتف الذكي التعايش معًا؟

تقييم التقنيات واللوائح المتعلقة بحماية البيانات الشخصية على أجهزة أندرويد (Android) وآي أو إس (iOS)

أركادي يروخيموفيتش *(Arkady Yerukhimovich)*، ريبيكا بالباكو *(Rebecca Balebako)*، آن بوستيد *(Anne Boustead)*، روبرت ك. كونينغهام *(Robert K. Cunningham)*، ويليام ويسلر الرابع *(William Welser IV)*، ريتشارد هوسلي *(Richard Housley)*، ريتشارد شاي *(Richard Shay)*، تشاد سبنسكي *(Chad Spensky)*، كارلين د. ستانلي *(Karlyn D. Stanley)*، جيفري ستيوارت *(Jeffrey Stewart)*، آري تراختنبرغ *(Ari Trachtenberg)*، زيف ونكلمان *(Zev Winkelman)*

النتائج الرئيسية

- يختلف نظام أندرويد (Android) الذي تصدره شركة جوجل (Google) بشكل كبير عن نظام آي أو إس (iOS) الذي تصدره شركة أبل (Apple). يعود سبب ذلك إلى حد كبير إلى طريقة أداء الأعمال الخاص بكلتا الشركتين. لكن في الوقت نفسه، يوجد بعض التشابه فيما يتعلق بأدوات وطرق حماية كلا النظامين. أصبح نظام أندرويد، على سبيل المثال، يطلب إذن المستخدم عند احتياج التطبيق لأداء مهمة ما، وهو ما كان يقوم به نظام آي أو إس لسنوات. كما أن كلاهما يضم تشفيراً أقوى من ذي قبل.
- يمكن لبعض التطبيقات على نظام أندرويد ألا تطلب أذونات، لكنها قادرة في الوقت نفسه على تسجيل المحادثات المنطوقة والوصول إلى عدد من البيانات الحساسة الكفيلة بتحديد هوية الهاتف بدقة، كما أنها قد تملك القدرة على إحداث أخطاء قليلة الخطورة في النظام.
- رغم استخدام معظم البنوك التشفير بشكل صحيح، إلا أن تطبيقات بعضها لا تزال تُظهر أخطاءً كبيرة، في الوقت الذي ينقل العديد من البنوك معلومات أكثر مما هو لازم.
- نقترح أداةً تستند إلى دورة حياة البيانات و"مبادئ ممارسات المعلومات العادلة" (Fair Information Practice Principles). ستسمح هذه الأداة لصانعي السياسات بتحليل الثغرات ونقاط القوة في حماية الخصوصية في الهواتف الذكية خلال كل مرحلة من مراحل دورة حياة بيانات الهاتف.

الملخص ■ بات من الضروري على واضعي السياسات التصدي للقضايا المتعلقة بأمن الهواتف الذكية وخصوصيتها في ظل انتشارها في كل مكان في العالم؛ إذ تُظهر الدراسات رغبة، وحتى توقُّع، مستخدمي الهواتف الذكية في الحفاظ على خصوصيتهم (بليباكو، جونغ وآخرون، Balebako, Jung, et al 2013.؛ بويلز، سميث، ومادن، Boyles, Smith, and Madden, 2012؛ فيلت، إغلمان، وواغنر، Felt, Egelman, and Wagner 2012 ؛ وموسلوخوف وآخرون، Muslukhov et al., 2012). إلا أنه في الوقت نفسه، تتوقف الرغبات والتوقعات على امتلاك صانعي السياسات لنظرة أوسع للقوى التكنولوجية والاجتماعية والحكومية التي تشكل بيئة الهاتف الذكي المتطورة اليوم.

ومن أجل المساعدة في فهم ما سبق، قامت وكالة مشاريع الأبحاث المتطورة الدفاعية (DARPA) في عام 2015 بتشكيل فريق يتألف من باحثين من مختبر لينكولن التابع لمعهد ماساتشوستس للتكنولوجيا (MIT) ومن مؤسسة RAND بغرض تقييم خصوصية مستخدمي الهواتف الذكية من الناحيتين التكنولوجية والتنظيمية. يوثق هذا التقرير المنهج الذي اتبعه الفريق والاستنتاجات التي توصل إليها. كما يصف التقرير، فيما يتعلق بالجانب التقني، المراجعة الأدبية والتجارب التي أجراها فريق مختبر لينكولن في محاولته لتقصي حالة الخصوصية لمستخدمي منصتي الهواتف الذكية الرئيسيتين في عام 2015: نظام التشغيل أندرويد الذي تصدره شركة جوجل، ونظام آي أو إس الذي تصدره شركة أبل (والذي يعمل على أجهزة "آيفون" و"آيباد" التي تنتجها الشركة). أما من الناحية التنظيمية، فيتطرق هذا التقرير إلى المراجعة التي أجرتها مؤسسة RAND للآليات التي تتبعها الهيئات الأمريكية على مستوى البلاد فيما يتعلق بحماية الخصوصية في الولايات المتحدة الأمريكية. وأخيرًا، قدم الفريق أداةً لفهم الأمور التنظيمية المتعلقة بالخصوصية والتكنولوجيا.

لقد وجدنا أن التكنولوجيا لم تقم بما يكفي للحفاظ على خصوصية المستخدم رغم تحسنها مؤخرًا. كما تلعب وسائل الحماية التنظيمية المناسبة دورًا في حماية خصوصية مستخدمي الهواتف الذكية بشكل عام، مع العلم أن ثغرات كثيرة تنشأ حاليًا بين التشريعات والتكنولوجيا؛ إذ أنه لا يتم الربط بين الأمرين بشكل كافٍ لتوفير الحماية

المطلوبة. نؤمن بإمكانية استخدام صانعي السياسات للأداة التي طورها فريق المشروع بغرض تحديد العديد من هذه الثغرات، حيث ستساعد هذه الأداة القائمة على مصفوفة صانعي السياسات على تحديد الاتجاهات الخاصة بالأبحاث المستقبلية وتقييم أثر الحلول التقنية والتنظيمية التي طُبقت أو سوف تُطبق من خلال الجمع بين المكونات التقنية والتنظيمية المرتبطة بخصوصية الهاتف الذكي.

مقدمة

أعلن العديد من المتابعين المعروفين لعالم التكنولوجيا عن موت الخصوصية، مثل سكوت مكنيلي (Scott McNealy)، مؤسس شركة Sun Microsystems الذي أطلق تصريحًا شهيرًا في عام 1999 قال فيه: «لم يعد لديك خصوصية... عليك تقبّل ذلك». كما أطلق آخرون مؤخرًا تصريحات مماثلة تتعلق بوفاة الخصوصية مثل مارغو سيلتزر (Margo Seltzer) من المنتدى الاقتصادي العالمي حيث قالت، «لم يعد من الممكن العودة إلى الخصوصية التي كنا نعرفها في الماضي.... كما ماتت الطريقة التي كنا نفكر فيها بالخصوصية». صحيح أن هذه التصريحات، وغيرها، نالت الكثير من الانتباه، إلا أن السؤال كان دائمًا متصلًا بمدى دقتها، وفيما إذا كان موت الخصوصية من الأمور التي تهم المستخدمين.

يرغب الأمريكيون بوضوح في الخصوصية كما يتضح من عدة استطلاعات حديثة أجراها مركز أبحاث بيو (Pew Research Center) (بويلز، سميث، ومادن، Boyles, Smith, and Madden, 2012؛ ومادن وراياني، Madden and Rainie, 2015). أشارت غالبية الأمريكيين الذين شملهم الاستطلاع إلى قيامهم بتجنب استخدام تطبيق أو أكثر على هواتفهم الذكية لمخاوف متعلقة بالخصوصية، في حين أشار كثيرون إلى أهمية امتلاكهم إمكانية التحكم بمن يمكنه الوصول إلى بياناتهم الخاصة ورفضهم مراقبة الآخرين لهم دون إذن (بويلز، سميث، ومادن، Boyles, Smith, and, 2012 Madden؛ ومادن وراياني، Madden and Rainie, 2015).

إلا أن هذه الاستطلاعات إما تركت الخصوصية من دون تعريف محدد، أو وصفتها على أنها رغبة صاحب الهاتف الذكي في الحفاظ على قدرته على التحكم بكيفية مشاركة معلوماته الخاصة مع الآخرين. يكمن التحدي الماثل في تعريف الخصوصية في أن ما يُنظر إليه على أنه شخصي أو خاص يختلف باختلاف السياق والفرد، حيث قد يملك الأمريكيون مثلاً آراء مختلفة تجاه من يحصل على بياناتهم، وقد تختلف مخاوفهم المتعلقة بالخصوصية بحسب الجهة التي تحصل على المعلومات وفيما إذا كان يتم مشاركة هذه المعلومات مع حكومات أو شركات خاصة. أدركت شركات مثل جوجل وأبل المخاوف المتعلقة بالخصوصية واستجابت لذلك عبر استخدامها بوصفها ميزة تنافسية في السوق، إذ تقوم أبل على سبيل المثال بإصدار بيانات علنية بانتظام توضح فيه موقفها من الخصوصية لإغراء المستخدمين باستخدام

> لم يعد لديك خصوصية... عليك تقبّل ذلك
> – سكوت مكنيلي، (Scott McNealy)
> Sun Microsystems, 1999

منتجاتها، كما تعمل أبل وجوجل على وصف التكنولوجيا لديها بأنها تكنولوجيا تسعى للحفاظ على الخصوصية من أجل تمييز منتجاتها عن منتجات منافسيها.

تعتبر الخصوصية من الأمور المعقدة أينما كان السياق الذي تُعرض فيه (ويستن) (Westin, 1968)، وتزيد حالة الهواتف الذكية من هذا التعقيد، نظرًا لأنها تكنولوجيا جديدة مقارنةً بأجهزة الكمبيوتر المكتبي والمحمول، ولا تزال الحماية التي تقدمها في طور النمو. تشترك جهات عديدة مختلفة في بناء مكونات منصات الهواتف الذكية المختلفة، ولكل منها حوافز مختلفة. بالإضافة إلى ذلك، تميل الهواتف الذكية إلى جمع المعلومات بشكل مستمر نظرًا لأنها في حالة عمل طوال الوقت، ويحملها المستخدم معه في كل مكان، وتملك مجموعة واسعة من المستشعرات القادرة على جمع كميات هائلة محتملة من المعلومات الخاصة بالمستخدم. علاوة على ذلك، فإن حجم الشاشة الصغير لهذه الأجهزة يحد من إيصال الأفكار، وخصوصًا تلك المعقدة المتصلة بقضايا مثل الأمن والخصوصية (هاريس، غودمان، وترينور، Harris, Goodman, and Traynor, 2012).

ينظر هذا التقرير في حالة خصوصية الهاتف الذكي في مواجهة هذه الصعوبات والتعقيدات. نهدف هنا إلى فهم حالة الخصوصية في عالم الهواتف الذكية وتحديد الثغرات والفرص.

كما ننظر بشكل أكثر تحديدًا إلى وضع الخصوصية في نظام التشغيل آي أو إس الذي تصدره شركة أبل ونظام أندرويد الذي تصدره جوجل، واللذان يعملان على معظم أجهزة الهواتف المحمولة المتصلة بالإنترنت، التي غالبًا ما تُسمى بالهواتف الذكية وتُستخدم على نطاق واسع في كل مكان. نظرنا إلى موضوع الخصوصية في هاتين المنصتين مع الأخذ بعين الاعتبار الحماية التقنية والقوانين التنظيمية المتاحة. كما استخدمنا النتائج التي توصلنا إليها لتحديد الاتجاهات المستقبلية التي تتوجه إليها خصوصية الهاتف الذكي، ومعرفة الثغرات الكامنة بين التكنولوجيا والقوانين التنظيمية والتي يمكن أن تملؤها أبحاث مستقبلية أو ابتكارات تكنولوجية.

يجب أن يبدأ أي نقاش حول قضية الخصوصية على الهاتف الذكي بفهم كامل لأبعاد القضية. أولاً، لدينا الهاتف نفسه والذي يمتلك قدرات تكنولوجية ومستشعرات مختلفة قادرة على

جمع المعلومات. ثانيًا، علينا النظر إلى الوظيفة أو الفائدة التي يريد المستخدمون الحصول عليها لدى استخدامهم هذا الهاتف. بعبارة أخرى، هل ينوي المستخدم استخدامه لتصفح الإنترنت، أو لمباشرة الأعمال، أو للعب الألعاب؟ قد يؤدي كل استخدام إلى تفضيلات مختلفة في مستوى أبعاد قضية الخصوصية على الهاتف الذكي من قبل المستخدم، فضلًا عن نوعية المعلومات الخاصة التي ستُجمع وتُستخدم. وأخيرًا، علينا النظر في نماذج الأعمال الخاصة بمقدمي مختلف الخدمات الموجودة على الهاتف. تشمل القائمة هنا مصنّعي الهاتف، ومصنّعي نظام التشغيل، وشركات الاتصالات، ومطوري التطبيقات، وغيرهم. تختلف الطريقة التي تكسب بها كل مجموعة المال من الخدمات التي تقدمها اختلافًا كبيرًا، ولكل واحدة منها تبعات مختلفة على خصوصية المستخدم. على سبيل المثال، تعد جوجل شركة تكنولوجيا تستمد غالبية إيراداتها من الإعلانات التي تعتمد بدورها على بيانات جُمعت عن المستخدمين. وبدلاً من أن تقوم شركة جوجل بتصنيع أجهزتها الخاصة، فإنها تعمد إلى تشغيل أنظمتها التشغيلية على أجهزة تصنعها شركات متعددة، ما يتيح لخدماتها وإعلاناتهم أوسع انتشار ممكن. أما شركة أبل فهي تعمل بشكل أساسي على تصنيع الأجهزة وتجني معظم أموالها من بيعها (والتي بدورها تأتي مُحمّلة بنظام آي أو إس). أما فيما يتعلق بمطوري التطبيقات، فتأتي قدرتهم على جني الأموال من خلال دمج مكتبات الإعلانات في تطبيقاتهم، وهو ما قد يتطلب أحيانًا وصولًا إلى بيانات خاصة قد لا تكون ضرورية لمهام البرنامج ووظيفته الأصلية.

يجب علينا أخذ كل ما سبق بعين الاعتبار عند دراستنا للأدوات المستخدمة لضمان الخصوصية في الهاتف الذكي. هناك أولًا تكنولوجيا الحفاظ على الخصوصية، مثل تكنولوجيا التشفير، وتكنولوجيا العزل (والتي تعمل على عزل التعليمات البرمجية لكل تطبيق عن الآخر)، إضافة إلى نموذج الأذونات الذي يهدف إلى التحكم بما يمكن جمعه من معلومات المستخدم الخاصة (وحماية تلك البيانات بعد جمعها). ثانيًا، هناك اللوائح التنظيمية المختلفة لتعزيز الخصوصية، كالنصوص القانونية والنصوص المتصلة بالعقود والآليات السياسية، التي تهدف إلى حماية خصوصية الأفراد عبر فرض قواعد تتصل بنوع البيانات الخاصة التي يمكن جمعها وكيفية استخدامها.

بالتالي، من المهم النظر في التداخل بين هاتين الآليتين لحماية الخصوصية. كما يتوجب على مطوري التكنولوجيا فهم اللوائح التنظيمية القائمة المتعلقة بالحماية لضمان التزامهم بالسياسات والمعايير المعنية. كما يجب على الآليات التنظيمية بدورها النظر إلى ما يمكن تحقيقه ومدى قابليته للتنفيذ من الناحية التكنولوجية.

دورة حياة البيانات

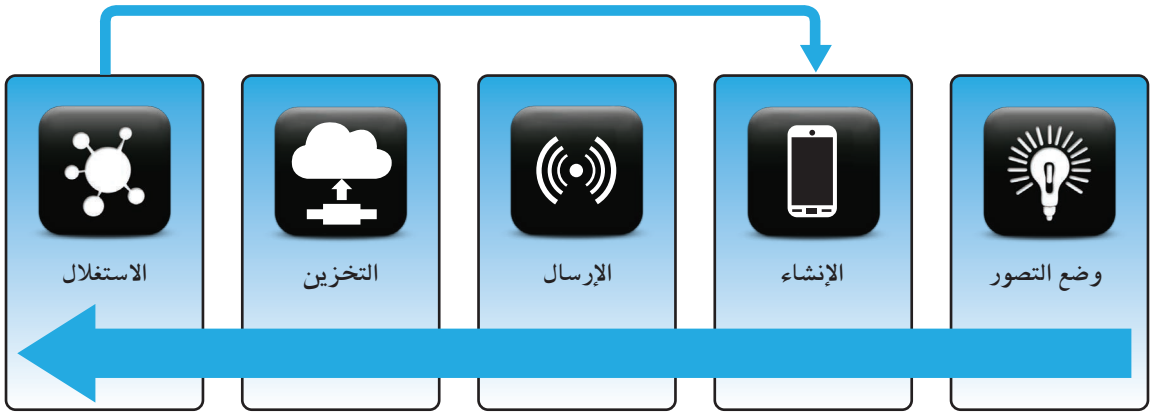
تمثل «دورة حياة البيانات» إحدى الطرق المفيدة في مساعدتنا على التفكير في كيفية حماية بياناتنا أثناء استخدامنا للهواتف الذكية. لم تكن مؤسسة RAND أول من أدرك أهمية فهم دورة حياة البيانات في الخصوصية. على سبيل المثال، يشير مفهوم «الخصوصية تبعًا للتصميم» (Privacy by Design) (كافوكيان، Cavoukian, 2009) إلى عملية دمج إجراءات حماية الخصوصية في الأنظمة من أجل توفير حماية للخصوصية وأمان طوال دورة حياة البيانات، إلا أنها في الوقت ذاته لا تحدد ما هي هذه الدورة. قامت مؤسسة RAND في هذا التقرير بتجزئة دورة حياة البيانات إلى أطوار تُحدد أي المعلومات بحاجة إلى حماية، ويتم عرضها في الشكل 1.

لتحديد مراحل دورة حياة البيانات عدد من الفوائد، إذ يسمح لمصمم المنصة بمعرفة إذا ما كانت الخصوصية محمية في كل مرحلة من تلك المراحل، كما أنه يعطي الجهات ذات العلاقة، من مختلف التخصصات، أرضية مشتركة تسمح لمن يعملون على عناصر مختلفة من المنظومة تحديد المرحلة التي تعمل فيها التكنولوجيا التي يقدمونها من مراحل دورة حياة البيانات هذه. في الوقت نفسه، تعتبر دورة حياة البيانات مفهومًا مرنًا رغم سماحه بتحديد الأطوار المتعلقة بنظام معين وتوفيره المصطلحات الخاصة بالمراحل المختلفة فيه. لا تعتبر دورة حياة البيانات مفهومًا مشترطًا جامدًا أو تعريفًا رسميًا، إذ يمكن للجهات ذات العلاقة اتخاذ القرارات ضمن كل مرحلة من مراحل دورة الحياة بشكل منفصل؛ على سبيل المثال، يمكن اتخاذ القرارات المتصلة بالحفاظ على الخصوصية في الأجهزة والبرامج خلال مرحلة وضع التصورات.

نحن بدورنا لا نقدم تعريفًا رسميًا للبيانات أو المعلومات، بل نراها كأي أمر يرغب المستخدم في حمايته مثل البيانات المتصلة بموقعه الجغرافي أو سجلاته الصحية مثلًا.

«لم يعد من الممكن العودة إلى الخصوصية التي كنا نعرفها في الماضي.... كما ماتت الطريقة التي كنا نفكر فيها بالخصوصية»
– مارغو سيلتزر، المنتدى الاقتصادي العالمي، 2015

الشكل 1. دورة حياة البيانات



RAND *RR1393-1*

المراحل

تبدأ دورة حياة البيانات بمرحلة وضع التصور، وفيها تُتخذ القرارات الخاصة بحماية خصوصية المستخدم قبل إنشاء البيانات. في هذه المرحلة، توضع قواعد حول البيانات التي يمكن الوصول إليها وكيفية حمايتها، حيث يمكن خلال هذه المرحلة اتخاذ عدة قرارات تتعلق بشكلٍ وثيق بتصميم النظام وبنيته، وهي قرارات تُتخذ قبل إنشاء البيانات. تتضمن الأمثلة على ذلك تحديد المصنعين مثلًا ما المستشعرات التي سيحتويها الهاتف، وتحديد مطوري أنظمة التشغيل متى ستُطبق حالتا الحماية أو العزل في نظام التشغيل، والقرارات التي يتخذها مطورو التطبيقات بشأن كيفية عمل التطبيق ونموذج الأعمال الخاص به. يمكن تقسيم مرحلة وضع التصور إلى مجموعات فرعية منفصلة لا تتداخل عامةً، وتشمل تلك المراحل الفرعية القرارات الخاصة بإنشاء نظام التشغيل، وتلك المتعلقة بإنشاء متجر التطبيقات أو تصنيع الهواتف أو تطوير التطبيقات أو غير ذلك. من المهم إدراك أن كل ما سبق يحدث قبل إنشاء البيانات فعليًا.

تصف مرحلة الإنشاء القرارات المتخذة خلال قيام الهاتف الذكي بإنشاء البيانات و/أو التقاطها من البيئة المحيطة به. قد يكون المستخدمون في بعض أنظمة الهواتف الذكية الحالية قادرين مثلًا على اتخاذ القرارات خلال مرحلة إنشاء المعلومات إذا تم إخطارهم وقت التشغيل بأن بياناتهم تُجمع، وقُدم إليهم إشعارات تفيد بذلك تُعرف بإشعارات اللحظة الأخيرة. تختلف مرحلة الإنشاء عن مرحلة وضع التصور في وجود أكثر من سياق متصل بالبيانات التي يتم إنشاؤها وجمعها، فضلًا عن امتلاك فكرة أكبر حول القيمة المحتملة للبيانات التي تُجمع.

تحدث مرحلة الإرسال عند انتقال البيانات. عادة لا تُخزّن البيانات فقط على الهاتف، بل قد تنقل إلى أماكن تخزين أو يتم مشاركتها مع مستخدمين آخرين أو شركات أخرى. قد تشمل القرارات المتعلقة بهذه المرحلة نوع وسيلة النقل المستخدمة، مثلًا شبكة اتصالات لاسلكية أو شبكة Wi-Fi. كما قد تتضمن هذه المرحلة إدراج آليات مثل التشفير لمنع هجمات «الوسيط»، التي يحاول فيها المهاجمون التنصّت على البيانات، أو حتى تغيير وجهتها بالكامل بين الأطراف دون معرفتها.

تُحفظ البيانات في مرحلة التخزين في مكان التخزين. وفي النظام البيئي للهواتف الذكية، غالبًا ما يقوم مزودو خدمة التخزين السحابي بتخزين البيانات على شبكات التخزين السحابية. ويتّخذ هؤلاء المزودون في هذه المرحلة قرارات تتعلق بكيفية تنظيم البيانات وحفظها، مثل مكان تخزين البيانات، وتاريخ انتهاء صلاحيتها، ومن يمكنه الوصول إليها.

كما يمكن تخزين البيانات على الجهاز، إما كنسخة إضافية إلى تلك المخزنة على السحابة، أو بدلاً منها. في حالة تخزين البيانات على الجهاز فقط، عندما تكون البيانات مخزنة في مكان إنشائها، يجوز تخطي مرحلة إرسال. وكما نوهنا سابقًا، فإن دورة حياة البيانات مرنة بما يكفي للسماح بذلك.

قد تدخل البيانات مرحلة الاستغلال، ويعني ذلك في هذا السياق تحليلها أو استخدامها، أحيانًا بطرق حُددت مسبقًا وأحيانًا أخرى بطرق جديدة نشأت من انصهار هذه البيانات مع أخرى. لا نعني بعبارة مرحلة الاستغلال في هذا السياق استغلال هذه البيانات في توجيه برمجيات خبيثة تنطوي على أنشطة ضارة أو مؤذية للمستخدم، بل نعني، مثلًا، قيام مطوري التطبيقات بتحليل البيانات لفهم كيفية استخدام المستخدمين لتطبيقاتهم، أو قيام معلنين خارجيين باستخدام مجموعة بيانات واحدة أو متعددة لتحديد الإعلانات التي سيقدمونها لهذا الهاتف.

يعرض الشكل 1 أيضًا وجود رابط يرجع من مرحلة الاستغلال إلى مرحلة الإنشاء ويعبّر عن الحالة التي قد تعود فيها البيانات من مرحلة الاستغلال كمعلومات جديدة سيتم إنشاؤها، مثل استنتاجات أو ملفات تعريفية جديدة للمستخدمين. نادرًا ما تختفي البيانات عن الوجود نظرًا لأنها تُنسخ ويعاد إرسالها واستغلالها عدة مرات.[1] كما أنها لا تملك عمرًا محددًا وقد تبقى موجودة بأشكال مختلفة لفترات زمنية غير محددة. يمكن أن يتم نسخ البيانات ومشاركتها في مرحلة الاستغلال. وغالبًا ما يتم مشاركة هذه البيانات بعيدًا عن التطبيقات مع جهات خارجية مختلفة مثل شركات الإعلان أو شركات التحليل أو جهة حكومية،

منهجية البحث

ركز هذا البحث على التكنولوجيا واللوائح التنظيمية المستخدمة لحماية الخصوصية المتعلقة بالهواتف الذكية، وحاول فهم كيفية تداخلها لتوفير الحماية للمستخدمين. تُعتبر هذه المقاربة ثنائية الجانب ضرورية نظرًا لأن على مطوري الأنظمة، وعلى الهيئات التنظيمية، أخذ الجانبين بعين الاعتبار لإنجاح انتقال أي نظام لحماية خصوصية من مرحلة الأبحاث إلى مرحلة النشر الواسع وتبني السوق له. ومن أجل فهم هذين الجانبين المتعلقين بخصوصية الهاتف الذكي فهمًا أفضل، قدمنا تفسيرنا المتعلق بدورة حياة البيانات لتحديد المخاوف المتعلقة بالخصوصية والقرارات وصناع القرار المشاركين في كل جزء من عمليات الهاتف الذكي.

التكنولوجيا. قمنا بتقييم تكنولوجيا الحفاظ على الخصوصية المتوفرة على منصتي الهواتف الذكية المهيمنتين: نظام التشغيل أندرويد الذي تصدره شركة جوجل وآي أو إس الذي تصدره شركة أبل. بدأنا بمراجعة عيّنات من متجر كل واحد منهما، ثم فحصنا نماذج الأذونات، ووضع الحماية، وتشفير البيانات. كما قمنا بتسليط الضوء على أوجه التشابه والاختلاف في الحماية التي تقدمها كل منصة من هاتين المنصتين وتأثيرها على خصوصية المستخدم.

قمنا أيضًا بتنفيذ عدة تجارب لتقييم مدى توافق تكنولوجيا الحفاظ على الخصوصية المتوفرة حاليًا مع أهدافها المعلنة، وتقصينا على وجه الخصوص مقدار البيانات الخاصة التي يمكن للتطبيقات الوصول إليها من دون طلب أي أذونات، إما عبر جمع النظام بيانات حساسة من التطبيق أو عبر فحص نظام واجهة برمجة التطبيقات (API) لاستخراج المعلومات الحساسة منه.

إضافة إلى ذلك، استقصينا فيما إذا كان التشفير يُستخدم بشكل مناسب لحماية البيانات الخاصة ضمن التطبيقات المصرفية وخلال دورة حياة البيانات لتوضيح الثغرات ونقاط القوة في الحماية.

اللوائح التنظيمية. قمنا بمراجعة آليات الإنفاذ التنظيمية المتاحة لحماية خصوصية المستهلك للتعرف على اللوائح التنظيمية المتعلقة بخصوصية الهواتف الذكية، حيث بدأنا بوصف بعض الأطر التي يمكن استخدامها لفهم العدد الهائل من القوانين الاتحادية والآليات التنظيمية لحماية الخصوصية في الولايات المتحدة. شمل ذلك النظر في "مبادئ ممارسات المعلومات العادلة" (FIPPS)، وهي مبادئ لحماية الخصوصية استخدمها المنظمون لعقود.

وحاولنا تحديد أي إطار عمل هو الأكثر كفاءة لتحديد الثغرات في حماية الخصوصية من الناحيتَين التنظيمية والتكنولوجية، واستخدمنا لهذا الغرض عدة معايير مثل الاكتمال، وقابلية التطبيق فيما يتعلق بالتكنولوجيا، وقابلية التطبيق فيما يتعلق باللوائح، لكن لم يستوفِ أي من الأطر تلك المعايير. وبغرض معالجة ذلك، قمنا باتخاذ خطوتين: تمثلت الأولى في تصويرنا ووصفنا لمراحل دورة حياة البيانات للهواتف الذكية التي تضع إطارًا مستمرًا لتحديد تكنولوجيات حماية الخصوصية وصناع القرار. ثانيًا، جمعنا دورة حياة البيانات مع "مبادئ ممارسات المعلومات العادلة" (FIPPs) لاستحداث أداة جديدة نشير إليها على أنها "مبادئ ممارسات المعلومات العادلة المتعلقة بدورة حياة البيانات" (DL-FIPPs) وتسمح للشخص بتحليل الثغرات ونقاط القوة في الحماية في كل خلية من المصفوفة.

ما يثير قلق المستخدمين (باليباكو، جونغ، وآخرون، Balebako, Jung, et al., 2013؛ ويوربان، هوفناغل، ولي Urban, Hoofnagle, and Li, 2012). تركز الجوانب التكنولوجية في هذا التقرير بشكل خاص على البيانات الموجودة على الجهاز. ستساعد المعلومات المذكورة في آخر هذا التقرير حول الجوانب التشريعية، وإطار العمل الثنائي الأبعاد، على النظر في كيفية مشاركة الجهات الخارجية البيانات وإعادة استخدامها.

قد تتخذ مجموعات مختلفة القرارات في كل مرحلة من مراحل دورة حياة البيانات. يعتبر فهم هذه الآلية أمرًا مهمًا لفهم الحالة التنظيمية على امتداد دورة حياة البيانات وذلك نظرًا لخضوع كل صانع قرار إلى قوانين أو عمليات رقابة مختلفة عن الآخر ومن هيئات تنظيمية مختلفة أيضًا. كما قد تؤثر مهارات صانعي القرار والموارد المتوفرة لهم على تدابير الحماية الفنية المعتمدة، ما يبرز أهمية تحديد صنّاع القرار لفهم أنواع حماية الخصوصية المطبقة فهمًا أفضل. على سبيل المثال، قد يفشل مطورو التطبيقات غير المتمتعين بخبرة أمنية في تطبيق التكنولوجيات التي تحافظ على الخصوصية بشكل صحيح (باليباكو، مارش، وآخرون، Balebako, Marsh, et al., 2014).

صناع القرار

يلعب العديد من صناع القرار دورًا معينًا على امتداد دورة حياة البيانات، وسيناقش هذا القسم صنّاع القرار بشكل عام وتوضيحي بسبب اعتماد قائمة صناع القرار الكاملة على التطبيق والمنصة المحددين. في مرحلة وضع التصور، يتخذ مطورو المنصة قرارات تتعلق بالأجهزة، مثل المستشعرات التي قد تتوفر في الجهاز، وهو

ما يؤثر على نوع البيانات التي يمكن جمعها عبر الهاتف. كما يتخذ مطورو المنصة أيضًا قرارات تتعلق ببنية نظام التشغيل التي يمكن أن تؤثر بدورها على الخصوصية والأمن. تتضمن الأمثلة على ما سبق تحديد إن كان سيُطبق التشفير على مستوى النظام، أو استخدام تقنية عزل التطبيقات عن بعضها. يتحكم متجر التطبيقات بالتطبيقات المتوفرة للتنزيل، وتؤثر مراجعات الأمن والخصوصية (أو عدم وجود مراجعات الخصوصية) التي يقدمها متجر التطبيقات في إمكانية تنزيل تطبيقات تخترق الخصوصية أو برامج خبيثة (شركة أبل، 2016؛ لوكهيمر، Lockheimer, 2012). يتخذ مطور التطبيق، خلال برمجته للتطبيق، الكثير من القرارات تجاه الوظائف التي ستقوم بجمع البيانات ونوع البيانات التي ستُجمع.

في مرحلة الإنشاء، يمكن للمستخدمين اختيار البيانات التي يمكن للجهاز الحصول عليها من خلال إعطاء الأذونات اللازمة. قد يطلب مطورو التطبيقات والمعلنين بيانات وافق عليها المستخدم سابقًا؛ كما يمكن للمعلنين ومطوري التطبيقات التحكم في معدل تكرار جمع البيانات، وهو أمر لا يعرفه معظم المستخدمين الذين وافقوا على جمع التطبيقات لبياناتهم.

في مرحلة الإرسال، قد يتغير صناع القرار تبعًا لطريقة الإرسال. على سبيل المثال، قد يستخدم مزود الاتصالات تقنيات مختلفة ويمكنه اتباع قواعد تنظيمية مختلفة عن مزود خدمة الإنترنت. بالتالي قد تختلف الآثار المترتبة على خصوصية نقل البيانات عبر الإنترنت (عبر شبكة لاسلكية أو سلكية) عن تلك المترتبة على نقل البيانات باستخدام شبكة خلوية.

في مرحلة التخزين، إذا تم تخزين البيانات على السحابة، قد يقوم مزود خدمة السحابة باتخاذ القرارات التي تؤثر على خصوصية البيانات حيث قد تشمل القرارات التقنية من يمكنه التحكم في الوصول والمعايير التي يتبعها، وما إذا كان التشفير أو الحذف متاحين. قد تؤثر قرارات أخرى على طريقة التنظيم. على سبيل المثال، قد يكون لموقع الخوادم السحابية أثر، وقد يكون لدى بلدان ودول مختلفة لوائح مختلفة بشأن خصوصية البيانات. وفي حال عدم تخزين البيانات على السحابة فقط أو في حال تخزينها على الهاتف فقط، فقد يتم إشراك جهات معنية أخرى.

تعتبر مرحلة الاستغلال مثيرة للاهتمام بشكل خاص، حيث قد ترغب الجهات المعنية المختلفة في الوصول إلى البيانات وقد تقرر استخدامها بطرق مختلفة. يتوقع العديد من مستخدمي الهواتف الذكية وصول المطور إلى البيانات التي تم جمعها، واستخدامها لغرض تحسين التطبيق (باليباكو، جونغ، وآخرون Balebako, Jung, et al. 2013). مع ذلك، قد لا يتوقع مستخدمو الهواتف الذكية من مطوري التطبيقات إعادة بيع بياناتهم إلى أطراف أخرى. يمكن للمعلنين الحصول على الملف الشخصي الخاص بالمستخدم خلال مرحلة الاستغلال، وقد تؤثر هذه الملفات الشخصية في الإعلانات التي يتعرض لها المستخدمون. كما قد تطلب الحكومة الوصول إلى المعلومات، ما قد يسبب مخاوف حول الخصوصية لدى المستخدمين.

عمومًا، تمثل دورة حياة البيانات في بيانات الهاتف الذكي وسيلة للنظر في كيفية حماية الخصوصية في منظومة الهاتف الذكي. وهي تتيح فرصة لشركات التكنولوجيا والهيئات التنظيمية للنظر في توفر الحماية طوال دورة الحياة أو لتحديد كيفية تناسب التكنولوجيا أو التنظيم في مرحلة معينة من دورة الحياة.

تكنولوجيا الحفاظ على الخصوصية

تتوفر عدة تكنولوجيات تعمل على الحفاظ على الخصوصية في كلتا المنصتين، وتشمل أدوات مثل نموذج سوق التطبيقات، ونماذج حصول التطبيق على أذونات لتنظيم عمله على الهاتف، والعزل، وتشفير كامل الجهاز، والتشفير خلال الإرسال لحماية البيانات التي يتم جمعها وتخزينها وإرسالها من خلال الهاتف، وتأمين بيئة موثوقة للإقلاع والتنفيذ لحماية الجهاز نفسه من الهجمات التي قد تؤدي إلى الوصول إلى البيانات الخاصة. وقد ركزنا على الآثار المتعلقة بخصوصية بيانات المستخدمين عند مقارنة الطريقة التي تنفذ بها طرق الحماية على أجهزة آي أو إس وأندرويد. وبشكل عام، فإن تقنيات الخصوصية التي تستخدمها هاتان المنصتان متقاربة، ولكن لا تزال بعض الاختلافات الجوهرية تظهر نتيجة وجود اختلافات جوهرية بين نظامي آي أو إس وأندرويد.

الأنظمة البيئية

يتمثل أحد أكبر الفروق بين نظامي آي أو إس وأندرويد في أن أبل هي الشركة الوحيدة التي تصنع أجهزة آيفون (iPhone)، في حين تسمح جوجل لشركات كثيرة لصناعة الأجهزة بتشغيل نظام أندرويد، ما يؤدي إلى عدة اختلافات مهمة في ما يتعلق بحماية الخصوصية.

يُصعّب سماح منظومة جوجل لعدة شركات بصناعة أجهزة متنوعة من تصحيح الأنظمة الحالية نظرًا لوجود عدة إصدارات لنظام التشغيل يجب تصحيحها، وعدة أطراف مسؤولة عن تطبيق هذه التصحيحات، ما يؤدي إلى بطء عملية التصحيح. من ناحية أخرى، تكون أبل قادرة في أي وقت على إرسال تصحيحات لجميع الأجهزة التي تعمل بنظام آي أو إس. ويؤثر ذلك على خصوصية المستخدم إذ من المرجح أن تظل نقاط الضعف المحتملة المعروفة التي قد تعرض البيانات الخاصة إلى الخطر لفترة أطول في منظومة جوجل (فيداس، فوتيبكا، وكريستين، Vidas, Votipka, and Christin, 2011).

إضافة إلى ما سبق، نظرًا لسماح جوجل للشركات بتصنيع أجهزتها الخاصة، فإن هناك إمكانية لقيام هذه الشركات المختلفة بإضافة تطبيقاتها الخاصة إلى نظام أندرويد الأساسي، وإجبار المستخدمين على تثبيتها على هواتفهم لاستخدام خدماتها. غالبًا ما تسمح هذه التطبيقات، التي يُشار إليها غالبًا باسم «البرامج غير المرغوب فيها» (Bloatware) (مكدانيال، McDaniel, 2012) للمزودين بجمع كميات كبيرة من بيانات المستخدمين الشخصية

لاستخدامها لأغراضهم الخاصة.

من ناحية أخرى، تعد أبل المزود الوحيد لكل الأجهزة التي تعمل بنظام آي أو إس، ما يقلل من تنوع التطبيقات المثبتة مسبقًا (وخصوصًا تلك التي يعتبرها البعض برامج غير مرغوب فيها) على الأجهزة ومواردها. ولكن لنظام أبل المركزي ثمنه. نظراً لأن أبل هي المزود الوحيد لنظام التشغيل آي أو إس، فإن أي ثغرة أمنية في نظام التشغيل ذاك ستؤثر على البيانات الخاصة لجميع مستخدمي هذه الأجهزة لكونها تعمل على نفس نظام التشغيل، في حين قد يتجنب نظام أندرويد حصول ذلك لهذا نظرًا لتنوع إصداراته مع تنوع الشركات المصنّعة للأجهزة.

خلاصة القول هو أن نموذج آي أو إس المركزي يتمتع بقدرة أفضل على سرعة تصحيح الثغرات وحماية الخصوصية، إلا أن أي ثغرة تظهر فيه ستصيب شريحة كبيرة من المستخدمين.

متجر التطبيقات

تنعكس الاختلافات بين نظامَي التشغيل في متاجر التطبيقات أيضًا حيث تملك كل شركة النماذج الخاصة بها التي تتحكم بالتطبيقات التي يُسمح بتثبيتها وتشغيلها على أجهزة المستخدم. يحاول نظاما آي أو إس وأندرويد تحليل جميع التطبيقات المُضافة في متجر كل منهما ويستخدمان لهذا الغرض التحليلات الثابتة والديناميكية واليدوية للتأكد من عمل التطبيق على النحو المعلن عنه والمنصوص عليه وضمان، إلى حد ما، عدم احتوائه على أي تطبيقات خبيثة. إلا أن جوجل، كما هي حالة نظامها التشغيلي عامة، لا تملك سيطرة كاملة على التطبيقات المتوافقة مع أندرويد وتسمح للمستخدمين بتثبيت تطبيقات من مصادر غير معروفة حتى لو رفضها متجر التطبيقات (تقرير شركة جوجل: مراجعة سنوية لأمن نظام أندرويد لعام 2014، Google Report: Android Security 2014 Year in Review, 2014)، ما قد يسمح، من ضمن أمور أخرى، بتثبيت تطبيقات قد لا تحافظ على البيانات الخاصة وتحميها بالصورة المرجوة. وفي حين يعمل نظاما آي أو إس وأندرويد على اعتماد نموذج «عدم الثقة والتحقق» ("distrust and verify") في تعاملهما مع التطبيقات، يبقى الفرق الأساسي بينهما في مستوى التحكم الذي يتمتعان به.

نماذج الأذونات

قمنا أيضًا بفحص نماذج الأذونات على الأجهزة التي تعمل بنظامي آي أو إس وأندرويد، والتي تتحكم في المعلومات التي يُسمح للتطبيق بجمعها. في حالة نظام أندرويد، كان على المستخدم، قبل إصدار نوجا (Nougat) (وهو أحدث إصدار للنظام) الموافقة على جميع الأذونات عند تثبيت التطبيق لأول مرة، في حين يتطلب نظام التشغيل آي أو إس إعطاء الإذن وقت التشغيل (كما في إشعارات اللحظة الأخيرة). يعني هذا أنه بإمكان مستخدمي أندرويد رؤية جميع الأذونات التي قد يحتاجها التطبيق خلال تثبيته، في حين يرى مستخدمو نظام آي أو إس مجموعة الأذونات اللازمة عند اختيار التطبيق الذي يريدون تثبيته.

اقترب نظام أندرويد في إصدار مارشميلو (Marshmallow) (إصدار سبق نوجا الحالي) من نموذج عمل نظام آي أو إس، إذ بات على التطبيقات طلب مجموعات معينة من الأذونات الإضافية حسب الحاجة، بدلاً من توفر جميع الأذونات معًا عند التثبيت لأول مرة. تختلف عملية الموافقة على الأذونات وقت التشغيل إلى حد ما بين نظامي آي أو إس وأندرويد، حيث يطلب نظام أندرويد من المستخدم الموافقة فقط على الأذونات التي يعتبرها «خطيرة» (تايلور، Taylor, 2015) لطلبها معلومات المستخدم الخاصة، لكن في الوقت نفسه، لا تشمل هذه الأذونات الخطيرة أذونات مثل ضبط المنبه أو الوصول إلى الإنترنت. يطلب نظام آي أو إس الحصول على موافقات في حينه على أي قدرات محددة غير افتراضية مثل السماح بالتخزين على iCloud) (أتينزا وآخرون ,.Atienza et al 2015).

وأخيراً، يفرض نظاما آي أو إس وأندرويد قيودًا على نماذج أذوناتهما باسم سهولة الاستخدام، إذ يضع أندرويد مثلًا الأذونات ضمن مجموعات، بشكلٍ يعطي الموافقة على كامل الأذونات في المجموعة لدى الموافقة على إذن واحد. أما نظام آي أو إس، فيسمح ببعض الأذونات الافتراضية التي تمكّن الوصول إلى التطبيق دون الحاجة إلى موافقة المستخدم. غير أن كلا الإجراءين يحدان من مستوى تحكم مستخدم الهاتف في بياناته الخاصة.

تقنيات العزل والتشفير

يستخدم كلا النظامين العزل والتشفير لحماية بيانات الهاتف. تحاول تقنية العزل (Sandboxing) تخصيص مكان مستقل لكل تطبيق لمنعه من الوصول إلى بيانات جمعها تطبيق آخر ويُحتمل أن تكون حساسة. صحيح أن النظامين يستخدمان تقنيات مختلفة، إلا أنهما يوفران مستويات الحماية ذاتها.

كما يوفر كلا نظامي التشغيل إمكانية تشفير الجهاز لحمية البيانات التي تجمعها التطبيقات أثناء تخزينها على الهاتف. يقوم نظام آي أو إس بتشفير الجهاز بالكامل بشكل افتراضي، مما يضمن تشفير جميع البيانات طوال الوقت، في حين يقدم نظام أندرويد حاليًا التشفير كخيار؛ ما قد يعرّض البيانات للخطر. إلا أن جوجل تخطط لجعل التشفير افتراضيًا على نظام أندرويد أيضاً. كما يستخدم آي أو إس وأندرويد تقنية «تسجيل المفتاح المدعومة من الأجهزة» (hardware-backed key signing) لمنع الهجمات التقليدية على مفاتيح التشفير.

تجارب لتقييم فعالية تكنولوجيا الحفاظ على الخصوصية

أجرى أعضاء فريق المشروع من مختبر لينكولن التابع لمعهد ماساتشوستس للتكنولوجيا عددًا من التجارب حاولوا فيها معرفة مدى جودة تقنيات حماية الخصوصية في تقديم الغرض المرجو منها، وهو حماية خصوصية المستخدم في العالم الحقيقي. وبشكل أكثر تحديدًا، أجرى الباحثون تجربتين مختلفتين لتقييم فعالية نموذج الأذونات عبر النظر في نوعية البيانات الخاصة التي يمكن لشخص ما الوصول إليها عبر تجاوز نموذج الأذونات من خلال «واجهة برمجة التطبيق» (API) الخاصة أو من خلال استغلال واجهة برمجة التطبيقات الحالية الموجودة في النظام. ومن أجل فهم نوعية المعلومات الخاصة التي يمكن لمخترقي الإنترنت الوصول إليها، أجرى فريق البحث العديد من التجارب لتقييم ما إذا كانت التطبيقات المختلفة تستخدم التشفير بشكل صحيح، وما هي المعلومات الخاصة التي قد تنقلها هذه التطبيقات.

ما هي المعلومات الخاصة التي يمكن لتطبيقات أندرويد الوصول إليها دون طلب إذن المستخدم؟

هَدَفت تجربتنا الأولى إلى تحديد المعلومات الخاصة التي يمكن للتطبيق العامل على نظام أندرويد الوصول إليها دون طلب أي أذونات من المستخدم. وبغرض قياس ذلك، قمنا بكتابة نص برمجي عمل على مسح المراجع العامة المتصلة بواجهة برمجة التطبيقات لنظام أندرويد لتحديد أنواع طلبات واجهة برمجة التطبيق التي لا تتطلب أي أذونات من المستخدم. بعد ذلك، تم غربلة القائمة التي تألفت من 36 ألف طلب تقريبًا يدويًا لتحديد تلك التي قد تشكل تسريبات محتملة للخصوصية. وقد وجدنا عددًا من التسريبات المتعلقة بالخصوصية. على سبيل المثال، اكتشفنا أن التطبيقات قادرة على تحديد ما تم تثبيته على الجهاز، وبالتالي معرفة هوية الهاتف بشكل دقيق وتحديد التطبيقات الضعيفة واكتشاف موقع البيانات الخاصة لاستغلالها. قد تكون معرفة هوية الجهاز بشكل دقيق (بصمة الجهاز) مصدر قلق كبير للخصوصية كونها تسمح بتحديد فريد للهاتف بطريقة قد لا يكون حتى مطور البرامج قد خطط لها. تسمح عملية تحديد بصمة الجهاز بمعرفة معلومات أكثر عن المستخدم أو الجهاز، مما يتيح جمع البيانات من مصادر مختلفة والخروج باستدلالات جديدة عن المستخدم تزيد حتى عما قد يتوقعه (تورناو، Turnow, 2012).

يتطلب إدراج حسابات فعلية على جهاز المستخدم أذونات خاصة، لكن في الوقت نفسه، لا تتطلب موثقات الحساب أي أذونات، وهي غالبًا ما تقدم معلومات عن الحسابات التي يملكها المستخدم، والتي منها ما قد يكون حساسًا وخاصًا، إلا أن بعض الخدمات قد تتشارك موثقات الحساب، ما قد يحد من الضرر الناتج عن هذه المعلومات.

إضافة إلى ما سبق، من الممكن للوصول إلى المدخلات التي يطلبها كل تطبيق من شبكة الإنترنت، والتي تشمل بيانات أرسلها أو استقبلها التطبيق. على سبيل المثال، تمكنا من معرفة عدد البايتات التي استهلكها Skype خلال فترة زمنية محددة، وهو ما قد يعتبر أمرًا فائق الحساسية. كما قد أظهرت أبحاث أخرى إمكانية استخدام تطبيقات تقنية نقل الصوت عبر بروتوكول الإنترنت (VoIP) لتحديد لغة الكلام (رايت، بالارد، مونروز، وآخرون، Wright, Ballard, Monrose, et al., 2007) وحتى الكشف عن عبارات محددة تم نطقها (رايت، بالارد، كول، وآخرون، Wright, Ballard, Coull, et al., 2010). يسمح ذلك للتطبيق بالتنصت على المحادثات الهاتفية الخاصة دون إذن، كما تسمح هذه القناة الجانبية أيضًا بمعرفة معلومات عن موقع المستخدم بشكل عام عن طريق مراقبة الحالات التي تقوم فيها تطبيقات الخرائط بتحميل أجزاء أماكن محددة من المدن التي يتحرك فيها المستخدم.

ما المعلومات الخاصة التي يمكن الوصول إليها باستغلال واجهة برمجة التطبيقات؟

قمنا بإجراء تجربة ثانية لتقييم المعلومات الخاصة التي يمكن الوصول إليها عن طريق استغلال واجهة برمجة التطبيقات الخاصة بالنظام، حيث قمنا – بشكل أكثر تحديدًا – بإنشاء أداة أطلقنا عليها اسم «تطبيق منعكس» (reflector app) تستخدم الصورة المنعكسة (مايكروسوفت، Microsoft, 2016). يعتبر استخدام الصورة المنعكسة مهمًا كوسيلة لمراقبة طلبات البرنامج عند عمله، ولقد استخدمنا الصورة المنعكسة لتحديد واستدعاء جميع الأمور والوسائل الممكنة التي قد تنشأ خلال عمليات الهاتف، وهو ما سمح لنا بإيجاد طرق إضافية يقوم من خلالها تطبيق ما بمشاركة البيانات الخاصة للمستخدم غير تلك المذكورة في وثائق واجهة برمجة التطبيقات. ترتبط هذه الطريقة ارتباطًا وثيقًا بالفحص العشوائي (fuzzing)، وهي تقنية يشيع استخدامها في اختبار ثغرات البرمجيات (ميلر، Miller, 2007)) ويتم فيها إدخال كميات كبيرة من البيانات العشوائية في شفرة البرنامج لمعرفة إن كان البرنامج سينهار. كنا نحن، على حد علمنا، أول من استخدم هذه التقنية للنظر في موضوع الخصوصية.

أدت هذه التجربة إلى عدة نتائج مثيرة للاهتمام فيما يتعلق بنظام أندرويد؛ أولها هو قدرة بعض المعلومات المتاحة للعموم، مثل المكتبات المشتركة وميزات النظام الأخرى، على تحديد «بصمة» الهاتف. ربما الأمر الأكثر إثارة للقلق هو القدرة على معرفة تخطيط لوحة المفاتيح على الهاتف، وهو ما قد يكشف عن لغة المستخدم المفضلة. ثانيًا، كشفنا عدة طرق محتملة خطيرة تسببت في أخطاء منخفضة المستوى في الجهاز، ولم يكتشفها الجهاز الافتراضي. قد تكون هذه العيوب ذات المستوى المنخفض مثار قلق أمني أكثر منه قلق متعلق بالخصوصية، إلا أنها تشير إلى احتمال وجود نقطة ضعف منخفضة المستوى يمكن لمخترق استغلالها. مع ذلك، لم نتمكن من الوصول إلى أي بيانات خاصة جدًا، مثل البيانات اللاسلكية أو أي طرق فريدة لتحديد بصمة الجهاز، وهو أمر إيجابي. وبالتالي،

بالرغم من وجود بعض المخاوف، إلا أن طريقة الصورة المنعكسة لم تكشف عن أي معلومات خاصة جدًا.

إلى أي مدى تستخدم التطبيقات التشفير في نقل البيانات أو نقل بيانات خاصة غير مهمة؟

ركزنا في تجربتنا ثالثة على التطبيقات المالية والمصرفية على اعتبار أنها الأكثر تطورًا نسبيًا والأكثر احتمالاً لاعتماد ممارسات أفضل في إدارة التشفير والبيانات الخاصة. قمنا على وجه التحديد بتحليل ٥٠ تطبيقًا مصرفيًا على أندرويد وآي أو إس لمعرفة مدى استخدام هذه التطبيقات للتشفير.

قمنا أولًا بالنظر إلى احتمالية قيام التطبيقات بالتحقق بشكل صحيح من شهادات الخادم المستخدم للتحقق من صحة الخادم وحماية اتصالاتها. يؤدي عدم القيام بذلك إلى فتح الباب أمام هجمات المخترقين التي يمكنها سرقة البيانات الخاصة عبر انتحال هوية خادم مصرفي. قامت غالبية التطبيقات المصرفية على نظامي أندرويد وآي أو إس بالتحقق من صحة الشهادات بشكل صحيح، لكننا وجدنا عددًا قليلًا من التطبيقات المصرفية التي لم تنفذ عملية التحقق من صحة الشهادات بشكل صحيح. يعني هذا أن عملية التحقق من الشهادة ما زالت عملية غير مباشرة، وهو ما يعني تعرض التطبيقات الأقل تطورًا إلى هذا الخطأ، ما يسمح باعتراض البيانات الخاصة أثناء انتقالها.

بالإضافة إلى ذلك، وفي حين أن التحقق من صحة الشهادات هو المعيار السائد حاليًا في الصناعة، إلا أنه يترك المستخدمين عرضة للهجوم القادر على تخريب عملية سلطة التصديق (certificate authority). من الأمثلة على المهاجمين الذين يمكنهم تخريب عملية سلطة التصديق نذكر الجهات الحكومية ومهاجمين مثل، ديجينوتار (DigiNotar)، وكومودو (Comodo)، وفيريساين (VeriSign). ونلاحظ وجود أمثلة مسبقة حول حالات تخريب سلطة التصديق لخلق شهادات وهمية (ويتني، Whitney, 2011). تعتبر «الشهادات المثبتة» (Pinning certificates) حاليًا وسيلة لتوفير المزيد من الضمانات أن نقطة النهاية التي يتحدث عنها التطبيق هي نقطة النهاية المتوقعة فعلًا. نلاحظ أن عددًا قليلًا من التطبيقات المصرفية تختار فعلًا استخدام هذا النهج الأقوى لإعطاء حماية إضافية لمستخدميها.

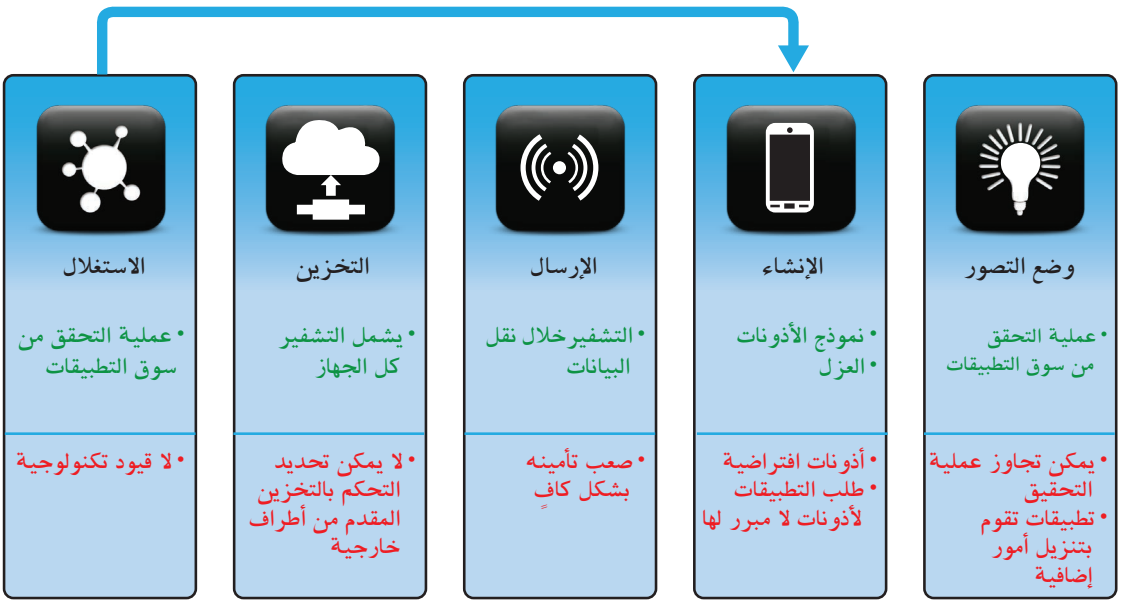
بعد ذلك، حصرنا وحللنا أنواع البيانات الخاصة التي تنتقل عن طريق هذه التطبيقات المصرفية خلال العمليات، حيث لاحظنا وجود نسبة لا بأس بها من التطبيقات على نظام التشغيل أندرويد التي يبدو أنها تنقل أمورًا تعريفية دائمة حول الجهاز، يمكن استخدامها لتحديد بصمة الجهاز. إضافة إلى ذلك، بدا وكأن عدة تطبيقات على نظامي التشغيل أندرويد وآي أو إس تقوم بنقل بيانات الموقع عندما لا يبدو ذلك ضروريًا، إذ لا تشمل لائحة بيانات الموقع الأذونات المتصلة بالخرائط. على وجه الخصوص، وجدنا تطبيقين على نظام التشغيل آي أو إس من أصل سبعة تطبيقات ترسل بيانات الموقع ينتظران الحصول على موافقة المستخدم على بيانات الموقع لأغراض تتعلق بالخرائط قبل إرسال البيانات دون استخدام الخرائط. يعني ذلك أساسًا أنهما يستفيدان من واقع أن المستخدم منح إمكانية الوصول إلى بيانات الموقع لغرض واحد، إلا أنهما استخدما البيانات لغرض آخر. علاوة على ذلك، يمكن التعرف على موقع المستخدم من معلومات أخرى تُرسل بخلاف تلك التي يرسلها التطبيق صراحةً عن موقع المستخدم. على سبيل المثال، تُرسل عدة تطبيقات ما يُعرف باسم «مُحدّد مجموعة الخدمات الأساسية» (Basic Service Set Identification)، الذي هو «عنوان تحكم دخول الوسائط – عنوان ماك» (MAC address) لنقطة الاتصال اللاسلكية بالإنترنت التي يستخدمها الجهاز وهو ما يجعل التطبيق قادرًا على كشف موقع المستخدم. ويشير نقل مثل هذه البيانات التعريفية أو غير الضرورية إلى احتمالية قيام هذه التطبيقات المصرفية باستخدام بيانات المستخدمين الخاصة في أغراض أخرى بخلاف تلك المعلنة، وهو ما يوحي بوجود ما قد ينال من خصوصية المستخدمين.

الوضع الحالي لتكنولوجيا حماية الخصوصية

عملنا على التحقق من كيفية حفاظ تكنولوجيا حماية الخصوصية المتوفرة على البيانات خلال دورة حياتها اعتمادًا على دورة حياة البيانات التي ذكرناها في الشكل 1 سابقًا، فضلاً عن محاولتنا تحديد بعض الثغرات التي قد تتواجد في وسائل الحماية الحالية. يعرض الشكل 2 النتائج التي توصلنا إليها حيث يشار إلى الحماية باللون الأخضر والثغرات باللون الأحمر.

في مرحلة وضع التصور، تحمي استراتيجية فحص سوق التطبيقات المستخدمين من خلال منع دخول أي تطبيقات خبيثة إليه، إلا أنه في الوقت ذاته، لا يمكننا النظر إلى تلك الحماية على أنها مثالية نظرًا لإمكانية تجاوز مرحلة الفحص، وقد تقوم التطبيقات التي تم فحصها بتنزيل تطبيقات ضارة ديناميكيًا خلال عملها على الجهاز. أما في مرحلة الإنشاء، فتحمي نماذج الأذونات وتقنية العزل خصوصية المستخدم من خلال تحديد نوع البيانات الخاصة التي يمكن للتطبيق جمعها وأي التطبيقات يمكنها الوصول إلى تلك البيانات. إلا أنه في الوقت ذاته، تملك هذه التكنولوجيا بعض أوجه القصور مع وجود إعدادات افتراضية للأذونات تعطي جميع التطبيقات إمكانية الوصول إلى بعض بيانات المستخدم، ومع طلب – وتلقي – العديد من التطبيقات أذونات إضافية أكثر مما هو لازم لعملها. أما في مرحلة الإرسال، فيوفر التشفير للمستخدمين مجموعة من الأدوات لحماية بياناتهم، إلا أنه صعب الاستخدام وغالبًا ما يُستخدم بشكل خاطئ، وهو ما يخلق بعض نقاط الضعف المحتملة. في مرحلة التخزين، يمكن استخدام التشفير على كامل الجهاز لحماية البيانات المخزنة على الهاتف الذكي، لكن حالما تنتقل البيانات من الهاتف إلى أي مكان تخزين آخر، يفقد المستخدمون أي ضمانات بحماية بياناتهم. أما في مرحلة الاستغلال

الشكل 2. حماية الخصوصية والثغرات في كل مرحلة من مراحل دورة حياة البيانات



RAND *RR1393-2*

الأخيرة، فهي غير مغطاة بأي تقنية حفاظ على الخصوصية، ما يعني غياب الضوابط تقريبًا على ما يمكن تحقيقه بالبيانات التي تم جمعها. في المحصلة، يوضح هذا التحليل أنه رغم محاولات التكنولوجيا حماية خصوصية المستخدم، لا نزال نجد عدة ثغرات فيما يتعلق بحماية الخصوصية الفعلية على امتداد دورة حياة البيانات.

آثار البرامج الخبيثة

إضافة إلى ما سبق، نظرنا بشكل موجز في آثار البرامج الخبيثة على بيئة الخصوصية، حيث قمنا على وجه التحديد، بمراجعة الدراسات الحالية لفهم أنواع البيانات الخاصة التي يود مؤلفو البرامج الخبيثة الحصول عليها واختلافها عن تلك التي تحاول التطبيقات غير الخبيثة الحصول عليها. فيما يتعلق بنظام أندرويد، توفرت بيانات كثيرة حول ما تقوم به البرمجيات الخبيثة، منها دراسة حملت عنوان «Andrubis بعد مليون تطبيق: دراسة لتصرفات البرامج الخبيثة الحالية لنظام أندرويد» «Andrubis-1,000,000 Apps Later: A View on Current Android Malware Behaviors» (ليندورفر وآخرون، Lindorfer et al., 2014) استخدمت تحليلًا ديناميكيًا وثابتاً لحوالي 400,000 ألف تطبيق برمجي خبيث مأخوذة من أماكن مختلفة. في الوقت نفسه، وجدنا معلومات أقل فيما يتعلق بالبرمجيات الخبيثة على نظام التشغيل آي أو إس، ما جعلنا نضطر إلى التركيز على قائمة صغيرة من البرامج الخبيثة المعروف وجودها على نظام التشغيل المشار إليه، ثم محاولة رؤية توافق البيانات الخاصة بها مع الإحصائيات التفصيلية المكثفة المتوفرة على نظام أندرويد.

اكتشفنا من هذا التحليل تركيز البرامج الخبيثة في نظامي التشغيل على الحصول على «المعرّفات الدائمة»، مثل «الهوية الدولية للأجهزة المتنقلة» (Mobile Station Equipment Identity) التي تميز جهازًا عن آخر، فضلًا عن وثائق تفويض أصحاب البرمجيات الخبيثة بهدف سرقة حسابات المستخدمين واستغلالها. كما بدا أن التطبيقات الخبيثة أقل تركيزًا على سرقة المعلومات الخاصة، مثل بيانات الموقع. والمثير للدهشة أن التطبيقات غير الخبيثة تكون أكثر عرضة لاستخدام هذه البيانات وتسريبها لأغراض مثل الإعلانات الموجهة.

نظرة عامة على تنفيذ اللوائح التنظيمية

كما وضّحنا في بداية التقرير، من المهم فهم البيئة التنظيمية المتعلقة بخصوصية المستهلك، إذ أنه بدون فهم تلك اللوائح، قد تفشل التكنولوجيا أو الأنظمة المتعلقة بحماية الخصوصية في تلبية المتطلبات القانونية والاجتماعية، وهو ما قد يتسبب في عدم انتقالها من مرحلة الأبحاث إلى مرحلة التوفر التجاري للمستهلكين. سنقوم هنا بتقديم لمحة موجزة عن بعض الوسائل التنظيمية التي قد تُستخدم لغرض حماية الخصوصية في منظومة الهاتف الذكي. لن نتطرق هنا إلى الحماية التي يوفرها الدستور الأمريكي للخصوصية من التدخلات الحكومية، بل سنركز على الحماية المقدمة للمستهلكين الذين قد يشعرون بأن خصوصيتهم منتهكة من التطبيقات أو تحليلات الشركات أو منصات المصنّعين التي تجمع البيانات عنهم. تركز هذه المناقشة على القانون الفدرالي المتعلق بحماية خصوصية المستهلك في الولايات المتحدة دون التطرق إلى قوانين الولايات الداخلية أو القوانين الدولية، والتي يمكن أن تكون بدورها مؤثرة أيضًا، مثل الجهود التي بذلها النائب العام في كاليفورنيا فيما يتعلق بموضوع خصوصية الهاتف الذكي

(ولاية كاليفورنيا، وزارة العدل، مكتب النائب العام، 2012a، 2012b، State of California Department of Justice, Office of the Attorney General)).

كانت إجراءات إنفاذ القانون التي قامت بها لجنة التجارة الفدرالية الأمريكية (FTC) مهمة بشكل خاص في حماية خصوصية المستهلكين في الولايات المتحدة، حيث تعتبر الجهة الأكثر نشاطًا في ضمان الامتثال لإجراءات حماية خصوصية المستهلك. تستخدم اللجنة سلطتها لحماية المستهلكين عبر فرضها على الشركات اتباع سياسات لحماية الخصوصية. كما تستخدم اللجنة، بحسب بياناتها، إنفاذ القانون والمبادرات السياسية وتثقيف المستهلكين وقطاع الأعمال لحماية معلومات المستهلكين الشخصية وضمان امتلاكهم المعرفة الكافية للاستفادة من الفوائد العديدة التي يقدمها السوق المتغير باستمرار (لجنة التجارة الاتحادية الأمريكية، U.S. Federal Trade Commission, 2000).

تنفيذ سياسات الخصوصية

بدأنا عملنا هنا مع مستخدمي الهواتف الذكية، ثم انتقلنا إلى مطور التطبيقات الذي يُنشئ تطبيقات الهواتف الذكية، ثم متاجر التطبيقات التي تسمح للمستخدمين بشراء هذه التطبيقات. ثمة اتفاقيات قائمة بين جميع هذه الجهات المختلفة، لكننا سنركز على نوع واحد من الاتفاقيات على وجه الخصوص، وهو سياسات الخصوصية التي ينشئها مطورو تطبيقات الهواتف المحمولة لإعلام المستخدمين بالمعلومات التي سيتم جمعها عنهم ومشاركتها مع الجهات الأخرى.

غير أنه لا يمكن اعتبار سياسات الخصوصية هذه مصدرًا سهلًا للحصول على المعلومات حول البيانات التي تجمعها تطبيقات الهواتف المحمولة عن المستخدمين، كما أنها قد لا تصف كيفية مشاركتها لهذه البيانات مع الجهات الخارجية – مثل المعلنين – فضلًا عن تقديمها معلومات شحيحة للمستخدمين تجاه مرحلة استغلال البيانات. فحص مختبر لينكولن 223 سياسة خصوصية على نظام أندرويد و126 سياسة خصوصية على نظام آي أو إس، حيث وجد أن على الشخص أن يكون في المتوسط طالبًا جامعيًا في سنته الثانية لكي يتمكن من فهم نص سياسة الخصوصية بشكل كامل، وأن ما يزيد عن 20% بقليل ممن لم يحصلوا على الشهادة الثانوية قادرون على فهم النص بالكامل. بعبارة أخرى، لا تؤدي سياسات الخصوصية الخاصة بالتطبيقات الغرض المرجو منها في تزويد المستخدمين بالمعرفة والخيار حول معلوماتهم الشخصية.

على الرغم من أن سياسات الخصوصية تمثل «اتفاقيات» بين المستخدمين ومطوري التطبيقات، لا تراها المحاكم مستوفية للمتطلبات القانونية التي تجعلها بمثابة «عقد قانوني». مع ذلك، يمكن للجنة التجارة الفدرالية استخدام قوانين حماية المستهلك لضمان التزام مطوري التطبيقات بسياسات الخصوصية التي يضعونها في تطبيقاتهم. بالتالي، وعلى الرغم من عدم كفاية اتفاقيات سياسية الخصوصية المذكورة، إلا أنها أصبحت جزءًا مهمًا من التزام لجنة التجارة الفدرالية بتنفيذ سياسات الخصوصية. هذا فضلًا عن وجود قوانين أكثر تحديدًا لحماية المستهلك يمكن للجنة استخدامها بهدف ضمان حماية بعض أنواع المعلومات أو المستخدمين.

على سبيل المثال، يهدف قانون «حماية خصوصية الأطفال على الإنترنت» (COPPA) إلى منع مشاركة المعلومات المتعلقة بالأطفال دون إذن آبائهم. بمعنى آخر، إذا قام مطور تطبيق بجمع معلومات حول طفل دون سن 13 عامًا من غير موافقة والديه، يمكن للجنة التجارة الفيدرالية تطبيق إجراءات قانونية ضده (قانون الولايات المتحدة، United States Code, 1998). بالتالي يضع قانون حماية خصوصية الأطفال خطًا يحمي المستخدمين من مطوري التطبيقات، في الوقت الذي يمكن أن تكون إجراءات الحماية تلك مدرجة في سياسة الخصوصية الخاصة بالتطبيق. إذا رأت اللجنة وجود حالة عدم التزام بقانون حماية الأطفال أو سياسة خصوصية التطبيق، فإنها قادرة على إطلاق آلية إنفاذ قانوني ضد تطبيق الهاتف المحمول غير الملتزم.

في أحد الأمثلة التي تشرح آلية عمل إنفاذ الخصوصية في الولايات المتحدة، قامت لجنة التجارة الفدرالية مؤخرًا باتخاذ إجراء قانوني ضد موقع «يالب» (Yelp) لجمعه معلوماتٍ عن الأطفال بصورة غير مناسبة. توصل الموقع إلى تسوية خارج إطار المحكمة مع لجنة التجارة الفدرالية دفع بموجبها غرامة مقدارها 450 ألف دولار (لجنة التجارة الفدرالية الأمريكية، غير مؤرخة، U.S. Federal Trade Commission, undated).

أطر عمل فحص اللوائح المتعلقة بالخصوصية

تمثّل هدفنا في تحديد نقاط القوة والضعف في اللوائح والتكنولوجيا المتعلقة بموضوع الحماية، حيث تقدم دورة حياة البيانات أحد الطرق لفحص هذه الحماية. لكن في الوقت نفسه، تتوفر أطر عمل أخرى أيضًا منها، على سبيل المثال، إمكانية النظر في أنواع البيانات المحمية لتحديد ما إذا كانت تتفق مع بعض القوانين القائمة المتعلقة بحماية المعلومات الشخصية مثل قوانين حماية المعلومات الصحية (قانون «قابلية التأمين الصحي وقابلية المحاسبة» (HIPAA)) أو قوانين حماية المعلومات الائتمانية المصرفية الخاصة بالمستهلك (مثل قانون «الإبلاغ الائتماني العادل» (Fair Credit Reporting Act)). كما أن هناك طريقة أخرى بديلة تتمثل في إمكانية التفكير بفئات الأشخاص المعنيين، مثل معرفة من يتحكم في البيانات أو من تنطبق عليه البيانات، حيث استخدمت هذه الطريقة في بعض القوانين مثل قانون «حماية خصوصية الأطفال على الإنترنت» (COPPA) وقانون «حقوق وخصوصية العملية التعليمية للأسرة» (Family Educational Rights and Privacy)، الذي يحمي معلومات الطلاب.

إلا أن هذه الأطر تتطرق إلى مجالات محددة. بمعنى آخر، تتطرق

إلى حماية الأشخاص والبيانات في مجال محدد ولا تقدم الحماية خارجه، وهو ما يعتبر ثغرة في موضوع الحماية.

مبادئ ممارسة المعلومات العادلة

كان إطار «مبادئ ممارسة المعلومات العادلة» (Fair Information Practice Principles) أحد الأُطر المستخدمة منذ فترة طويلة لفهم لوائح الخصوصية وتحديدها، وقد قدمت هذه المبادئ، التي وضعتها لجنة برئاسة الرائد في مجال الخصوصية ويليس وير(Willis Ware) في عام 1970 (وير، Ware, 2008)، الفكرة القائلة بأن ثمة العديد من الجوانب الواجب معالجتها لحماية خصوصية المستهلك. تتوفر نسخًا مختلفة من هذه المبادئ، كما أدرجتها عدة تشريعات في الولايات المتحدة وخارجها.

تعتمد لجنة التجارة الفدرالية، على سبيل المثال، على مبادئ ممارسة المعلومات العادلة، مستخدمةً تعريفًا محددًا لها مذكورًا في النص المُدرج في الصفحة التالية (لجنة التجارة الفدرالية الأمريكية، U.S. Federal Trade Commission, 2000).

وتجدر الإشارة إلى أن تعريف اللجنة للوصول يختلف عن ذلك الذي يعتمده مجتمع الأمن، إذ أنه لا يعتبر الوصول أمرًا يجب منعه لكنه أمر يطلبه المستخدمون، ما يسمح لهم برؤية البيانات الخاصة بهم وتصحيحها. أحد الأمثلة المألوفة في الولايات المتحدة هو قانون «توفير التقارير الائتمانية بشكل عادل» (قانون أمريكي، United States Code, 2012)، الذي يستلزم تمتع المستخدمين بإمكانية الوصول إلى التقارير الائتمانية الخاصة بهم وتصحيحها.

وصف لجنة التجارة الفدرالية لمبادئ ممارسة المعلومات العادلة

١. الإشعار: يجب على جامعي البيانات الكشف عن ممارساتهم المتعلقة بجمع المعلومات قبل البدء بجمع المعلومات الشخصية من المستهلكين.

٢. الاختيار: يجب أن يُعطى المستهلكون الخيار فيما إن كانوا يرغبون في أن تُجمع معلوماتهم الشخصية أم لا، وكيفية استخدامها والغايات التي ستُستخدم فيها إن كانت ستتجاوز تلك التي جُمعت لأجلها في المقام الأول.

٣. الوصول: يجب أن يتمكن المستهلكون من رؤية البيانات التي جُمعت عنهم والتحقق من دقتها واكتمالها.

٤. الأمن: يجب على جامعي البيانات اتخاذ خطوات معقولة لضمان أمان وسلامة المعلومات التي تُجمع عن المستخدمين وحمايتها من أي استخدام غير مصرح به.

٥. الإنفاذ: استخدام آلية موثوقة لفرض عقوبات تجاه عدم الامتثال لمبادئ ممارسة المعلومات العادلة.

أداة جديدة بشكل مصفوفة لتحديد نقاط القوة والضعف فيما يتعلق بالخصوصية

خلُص تحليلنا للأطر إلى أنه لا يمكن لمبادئ ممارسة المعلومات العادلة ولا دورة حياة البيانات وحدهما فهم الثغرات الموجودة في اللوائح أو التكنولوجيا بشكل مناسب. نتيجةً لذلك، قام فريق RAND، بالتعاون مع فريق مختبر لينكولن، بجمع مراحل دورة حياة البيانات وعناصر مبادئ ممارسة المعلومات العادلة في أداة بشكل مصفوفة ثنائية الأبعاد لتحديد نقاط القوة والضعف المتعلقة بالخصوصية.

يعرض الجدول 1 المصفوفة التي تجمع بين مراحل دورة الحياة (موزعة على أعمدة) ومبادئ ممارسة المعلومات العادلة (موزعة على صفوف). سنشير إلى هذه الأداة باسم «أداة دورة حياة البيانات ومبادئ ممارسة المعلومات العادلة (DL-FIPPS) [سندعوها اختصارًا هنا «بالمصفوفة»] للتعرف على دور دورة حياة البيانات ومبادئ الممارسة العادلة.

يمكن لمصمم أي نظام، من خلال التأمل في صفوف المصفوفة، التفكير في مدى توفر هذا النوع من الحماية بالنسبة لكل مرحلة من مراحل دورة حياة البيانات. على سبيل المثال، يمكن للمصمم دراسة ما إذا كانت الإشعارات التي تُقدم للمستخدم تغطي كل مرحلة من مراحل دورة حياة البيانات، كما يمكنه أيضًا دراسة ما إذا كانت إعدادات النظام توفر خيارات معرفية كافية للمستخدم في كل مرحلة من مراحل دورة حياة البيانات.

يعتبر الوصول من الأمور المثيرة للاهتمام أيضاً، إذ أن التطبيقات لم تركز بشكل عام على توفير إمكانية الوصول إلى البيانات المتعلقة بالمستخدم، وحاليًا تكون إمكانية الوصول موجودة في مرحلة التخزين فقط، إن كانت متوفرة. يمكننا أن نرى أمثلة حول ذلك في أداة تفضيلات الإعلانات التي تقدمها شركة جوجل والتي تخبر المستخدمين بالملف الشخصي الذي تم إنشاؤه عنهم، بما في ذلك تخمينات جوجل عن عمرهم وجنسهم. من ناحية أخرى، تم إيلاء اهتمام أقل لقدرة المستخدمين على الوصول إلى بياناتهم أو تصحيحها خلال مرحلة الإرسال، إلا أن هذا الأمر قد يزداد أهمية على اعتبار أن معلومات المستخدمين تُجمع طوال الوقت وتُنقل باستخدام المستشعرات، فضلًا عن أن القرارات والملاحظات بشأنها تتخذ في الحال.

يمكن بالتأكيد تقييم التكنولوجيا الأمنية في ضوء دورة حياة البيانات. يعتبر الالتزام القانوني لأي جانب من هذه الجوانب سؤالاً معلقًا نظرًا لإمكانية تدقيق بعض التكنولوجيا وجوانب الامتثال أكثر من غيرها. والسؤال الذي يجب أن يُسأل هنا هو كيف يمكن لنظام حماية الخصوصية التحقق من الامتثال للوائح في جميع مراحل دورة حياة البيانات وكيف يمكن تدقيق هذا الامتثال.

يؤكد إدراج مرحلة الاستغلال في دورة حياة البيانات على أهمية النظر في إمكانية وصول أطراف خارجية إلى البيانات وكيف يمكن (ما إذا كان من الممكن) احترام مبادئ ممارسات المعلومات العادلة. بالتالي، يسمح لنا هذا العمود بالنظر مثلًا إلى ما قد يحدث عندما يوفر التطبيق بيانات لأطراف مثل شركات الإعلان

الجدول 1. مصفوفة دورة حياة البيانات - ومبادئ ممارسة المعلومات العادلة

مراحل دورة حياة البيانات / مبادئ ممارسات المعلومات العادلة	وضع التصور	الإنشاء	النقل	التخزين	الاستغلال
الإشعار					
الاختبار					
الوصول					
الأمن					
الإنفاذ					
الإجمالي					

أو التحليل. وفي حالات إعادة بيع البيانات أو نسخها، هل يحصل المستخدمون على إشعار بالأمر وهل يتمتعون بإمكانية القبول أو الرفض؟ هل سيتمتع المستخدمون بحق الوصول إلى المعلومات التي يتم نقلها؟ وهل يتم النقل باستخدام أفضل الممارسات الأمنية؟ ثمة حاجة إلى مزيد من العمل حول كيفية إنفاذ الحماية في مرحلة الاستغلال.

استخدام الأداة

ولإثبات كيف يمكن استخدام المصفوفة، اقترحنا مثالين سمحا لنا بتحديد إما نقاط القوة أو نقاط الضعف في اللوائح أو التكنولوجيا المتعلقة بالخصوصية. في المثال الأول، الذي يوضح المجال المشترك بين الإنشاء والاختبار، في الخلية ذات اللون «البيج» في الجدول 2، نجد فجوة بين التكنولوجيا واللوائح. فمن ناحية، وفرت التكنولوجيا أذونات في وقت التشغيل تسمح للمستخدمين باختيار البيانات التي تُجمع عنهم، لكن من ناحية ثانية، يتطلب قانون حماية الأطفال امتلاك الآباء إمكانية اختيار ما يُجمع عن أطفالهم من بيانات، ممن تقل أعمارهم عن 13 عامًا. بالتالي، وفي حين توفر الأذونات في وقت التشغيل الخيار، إلا أنها لا تتطلب موافقة الوالدين، ويمكن للطفل الموافقة على الأذونات. نستنتج من ذلك أنه صحيح أن التكنولوجيا واللوائح تعالجان هذه المسألة، إلا أن هناك فجوة في طريقة تداخلهما في هذا الموضوع.

نظرنا في المثال الثاني، الظاهر في الخلية الأرجوانية، إلى المجال المشترك بين الإرسال والأمن. يمكننا أن نرى هنا الجهود المبذولة في الجانب التكنولوجي فيما يتعلق بتشفير البيانات خلال نقلها لمنع وصول المتطفلين إليها أو تعديلها. في الوقت نفسه، تنص اللوائح، مثل قانون «قابلية التأمين الصحي وقابلية المحاسبة»، على أنه يتعين على الكيانات المشمولة بالقانون تنفيذ تدابير تتعلق بحماية المعلومات المرسلة. في هذه الحالة، نرى أن التكنولوجيا تعمل على توفير الحماية المطلوبة بموجب تلك القوانين. صحيح أنه ليس بإمكاننا الادعاء بوجود حماية قوية ومعقولة، إلا أننا في الوقت ذاته لاحظنا وجود حماية أقوى للخصوصية في هذا المجال مقارنة بباقي المجالات.

وهكذا، يُظهر لنا هذان المثالان كيف يمكن استخدام الأداة لتحديد نقاط القوة والضعف في التكنولوجيا واللوائح فيما يتعلق بأنظمة الهواتف الذكية. وبدورنا نعتقد أن هذه المصفوفة ستكون فعالة بشكل خاص في تحديد الفجوات.

إلى أين تتجه الخصوصية فيما يخص الهواتف الذكية؟

من الناحية التكنولوجية، تتوفر منصتان لتشغيل الهواتف الذكية تملكان الكثير من القواسم المشتركة رغم اختلافهما الكبير. كما أدى اختلاف طريقة عملهما بدوره إلى اختلاف كبير في طريقة حماية نظام أندرويد ونظام آي أو إس للخصوصية على أجهزة الهواتف الذكية العاملة بهما وضمانها. في الوقت ذاته، تسمح نماذج الأذونات بالتحكم في البيانات التي يمكن للتطبيقات جمعها، كما أن كلا النظامين يعتمدان بشكل متزايد على التشفير لتأمين البيانات التي تُجمع.

فيما يتعلق باللوائح، يمتلك صانعو السياسات عدة خيارات لحماية الخصوصية، إذ قام بعضهم على سبيل المثال بتحميل المستخدم الجزء الأكبر من المسؤولية وإلزامه بالتعرف على الضرر الحاصل ضده وإثبات وقوعه فضلًا عن التعرف على مرتكب الجريمة. وقد يكون ذلك صعبًا بشكل كبير في حالات تجاوزات الخصوصية الحاصلة في العالم الرقمي حيث يكون الضرر غير ملموس، تمامًا كالشعور بالضعف، أو من الصعب تحديد المسؤول عن انتهاك الخصوصية.

الجدول 2. استخدام أداة "المصفوفة": مثالان

مراحل دورة حياة البيانات / مبادئ ممارسات المعلومات العادلة	وضع التصور	الإنشاء	النقل	التخزين	الاستغلال
الإشعار					
الاختبار		**تكنولوجيا الأذونات في وقت التشغيل:** لدى المستخدم خيار تجاه البيانات التي تُجمع عنه.	**قانون "حماية الأطفال":** يتطلب امتلاك الآباء إمكانية اختيار المعلومات التي تُجمع عن أطفالهم.		
		الثغرات: لا تتطلب الأذونات في وقت التشغيل موافقة الوالدين.			
الوصول					
الأمن			**تكنولوجيا التشفير خلال عملية النقل:** منع وصول المتطفلين إلى البيانات أو تعديلها.	**قانون قابلية التأمين الصحي وقابلية المحاسبة:** يتعين على الكيانات المشمولة اتخاذ تدابير لحماية المعلومات المرسلة.	
			نقاط القوة: تقدم التكنولوجيا الحماية التي يقتضيها القانون.		
الإنفاذ					
الإجمالي					

من غير المرجح حدوث إصلاح شامل للسياسات المتعلقة بالخصوصية في الولايات المتحدة على المدى القريب. تعتبر لجنة التجارة الفدرالية الجهة الحكومية الأمريكية الرئيسية العاملة على موضوع خصوصية المستهلك، ومن المرجح أن تستمر في دورها هذا في المستقبل القريب.

صحيح أن تكنولوجيا الحفاظ على الخصوصية تستمر في التحسن بشكل عام، إلا أنه لا يزال هناك بعض المشاكل التي لا يمكن حلها من خلال التكنولوجيا وحدها؛ بالتالي من الضروري فهم كيفية دمج التكنولوجيا مع اللوائح القائمة. يظهر العديد من الفجوات بين اللوائح والتكنولوجيا في الوقت الراهن، وهو ما يؤدي إلى وجود أوجه ضعف في الحماية وقابلية تطبيق اللوائح. قد تساعد «المصفوفة» التي قدمناها صنّاع السياسات على الحصول على نظرة ثاقبة على المسائل المتعلقة بالتكنولوجيا واللوائح الخاصة بالهواتف الذكية وتحديد نقاط القوة والضعف في النهج الحالي والمستقبلي فيما يتعلق بالسياسات.

ملاحظات

١. يهتم المستخدمون بأبعاد أخرى متعلقة بمشاركة البيانات، إلا أنها غير مدرجة في وصف دورة حياة البيانات التي قدمناها أعلاه، ومنها على سبيل المثال: تواتر تبادل البيانات، ومن يجري تقاسم البيانات معه، وما هي البيانات المستخدمة. نوصي بأخذ هذه الأبعاد بعين الاعتبار في كل مرحلة من مراحل دورة حياة البيانات.

٢. حاولنا أيضا إجراء نفس التحليل على أجهزة آي أو إس، إلا أن الهواتف ظلت تتعطل، ما منعنا من جمع أي معلومات مثيرة للاهتمام. نخطط للقيام بتقصي أكبر لهذا الأمر مستقبلاً.

٣. تتوفر عدة آليات قانونية أخرى (مثل المسؤولية التقصيرية، والقانون الجنائي، وقانون العقود) قد تكون مناسبة لحماية بعض الجوانب المتعلقة بالخصوصية ومنع انتهاك الآخرين لها، سواء كان تطبيقها بشكل خاص سيعتمد على الحقائق المقدمة. تتمثل إحدى الصعوبات المتعلقة باعتماد هذه الآليات في أنها تضع عبء الإثبات على عاتق المستخدم (المنتهكة خصوصيته) والذي عليه إثباتها فضلاً عن تحديد الجهة المسؤولة عن الانتهاك واستعداده لعرض هذه القضية أمام المحكمة. لا تضع عمليات الإنفاذ الخاصة بلجنة التجارة الفدرالية عبء الإثبات على المستخدم. إضافة إلى ذلك، تتوفر مصادر أخرى للآليات التنظيمية (مثل القانون الدولي أو قانون الولاية). يتضمن القانون الدولي مبادئ «الملاذ الآمن للخصوصية في الاتحاد الأوروبي– الولايات المتحدة (EU US Safe Harbor Privacy Principles) (انظر على سبيل المثال، «قائمة الملاذ الآمن الأمريكي–الأوروبي»، U.S.-EU Safe Harbor, 2015 List). صحيح أن هذه الآليات توفر حماية إضافية للخصوصية، إلا أن أبحاثنا أبقت تركيزها على الآليات التنظيمية الفدرالية الأمريكية.

٤. استخدمنا نسخة لجنة التجارة الفدرالية بدلاً من نسخة منظّمة التعاون الاقتصاديّ والتنمية من إصدار «مبادئ ممارسات المعلومات العادلة» (OECD Publishing, 2002) أو غيره من الإصدارات حيث انصب تركيزنا على اللوائح الفدرالية الأمريكية. وبينما يتسق ذلك مع تركيزنا، لاحظنا أن نسخة منظّمة التعاون الاقتصاديّ والتنمية تتضمن بعض المبادئ المتعلقة بالقيود المفروضة على جمع البيانات واستخدامها والتي قد تكون مفيدة أيضًا أثناء النظر في حماية الخصوصية بالكامل.

٥. نوينا أن تكون هذه المصفوفة الأداة التي يستخدمها أي شخص يطور أو يقيّم نظام حماية الخصوصية.

٦. انظر خيار «التحكم في إعلانات جوجل» (Control Your Google Ads)، غير مؤرخ، من أجل الوصول إلى الرابط الخاص بأداة التفضيلات الإعلانية.

المراجع

Apple, Inc., "iOS Security—Whitepaper," May 2016. As of July 7, 2016:
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Atienza, Audie A., Christina Zarcadoolas, Wendy Vaughon, Penelope Hughes, Vaishali Patel, Wen-Ying Sylvia Chou, and Joy Pritts, "Consumer Attitudes and Perceptions on mHealth Privacy and Security: Findings from a Mixed-Methods Study," *Journal of Health Communications*, Vol. 20, No. 6, 2015, pp. 673–679.

Balebako, Rebecca, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen, "'Little Brothers Watching You': Raising Awareness of Data Leaks on Spartphones," *ACM Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, Newcastle, United Kingdom, July 24–26, 2013.

Balebako, Rebecca, Abigail Marsh, Jialiu Lin, Jason I. Hong, and Lorrie Faith Cranor, "The Privacy and Security Behaviors of Smartphone App Developers," *Proceedings of Internet Society's NDSS Workshop on Usable Security (USEC)*, 2014.

Boyles, Jan Lauren, Aaron Smith, and Mary Madden, *Privacy and Data Management on Mobile Devices*, Pew Internet and American Life Project, September 5, 2012.

Cavoukian, Ann, "Privacy by Design: 7 Foundational Principles," Toronto, Canada: Information and Privacy Commissioner of Ontario, August 2009 (revised January 2011). As of October 20, 2015: http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

Felt, Andrew Porter, Serge Egelman, and David Wagner, "I've Got 99 Problems, but Vibration Ain't One: A Survey of Smartphone Users' Concerns," *Proceedings of the Second Annual ACM Conference on Computer and Communications Security (CCS) Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, Raleigh, N.C., October 19, 2012.

Google, "Control Your Google Ads," undated. As of July 8, 2016: https://www.google.com/settings/u/0/ads/authenticated

"Google Report: Android Security 2014 Year in Review," 2014. As of October 2015: https://static.googleusercontent.com/media/source.android.com/en//devices/tech/security/reports/Google_Android_Security_2014_Report_Final.pdf

Harris, Andrew, Seymour Goodman, and Patrick Traynor, "Privacy and Security Concerns Associated with Mobile Money Applications in Africa," *Washington Journal of Law, Technology, and Arts*, Vol. 8, No. 3, 2012, p. 245.

Lindorfer, Martina, Matthias Neugschwandtner, Lukas Weichselbaum, Yanick Fratantonio, Victor Van Der Veen, and Christian Platzer, "Andrubis-1,000,000 Apps Later: A View on Current Android Malware Behaviors," *Proceedings of the the Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*, September 11, 2014.

United States Code, Title 15, Sections 6501–6506, Children's Online Privacy Protection, 1998.

———, Title 15, Section 1681, Fair Credit Reporting Act, 2012.

Urban, Jennifer M., Chris Jay Hoofnagle, and Su Li, "Mobile Phones and Privacy," *UC Berkeley Public Law Research Paper Series*, No. 2103405, July 10, 2012.

"U.S.-EU Safe Harbor List," export.gov, 2015. As of July 14, 2016: https://safeharbor.export.gov/list.aspx

U.S. Federal Trade Commission, "Protecting Consumer Privacy," undated. As of October 20, 2015: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy

———, "Privacy Online: Fair Information Practices in the Electronic Marketplace, a Report to Congress," May 2000. As of November 19, 2015: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

Vidas, Timothy, Daniel Votipka, and Nicolas Christin, "All Your Droid Are Belong to Us: A Survey of Current Android Attacks," *WOOT '11 Proceedings of 5th USENIX Workshop on Offensive Technologies*, San Francisco, Calif., August 8–12, 2011, pp. 81–90.

Ware, Willis H., *RAND and the Information Evolution: A History in Essays and Vignettes*, Santa Monica, Calif.: RAND Corporation, CP-537-RC, 2008. As of July 7, 2016: http://www.rand.org/pubs/corporate_pubs/CP537.html

Westin, Alan F., "Privacy and Freedom," *Washington and Lee Law Review*, Vol. 25, No. 1, March 1, 1968, p. 166.

Whitney, Lance, "Comodohacker Returns in Diginotar Incident," *CNET*, September 6, 2011. As of July 7, 2016: http://www.cnet.com/news/comodohacker-returns-in-diginotar-incident/

Wright, Charles V., Lucas Ballard, Scott E. Coull, Fabian Monrose, and Gerald M. Masson, "Uncovering Spoken Phrases in Encrypted Voice over IP Conversations," *ACM Transactions on Information and System Security (TISSEC)*, Vol. 13, No. 4, December 2010, p. 35.

Wright, Charles V., Lucas Ballard, Fabian Monrose, and Gerald M. Masson, "Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?" *The 16th USENIX Security Symposium Proceedings*, 2007, p. 3.

Lockheimer, Hiroshi, "Android and Security," *Google Mobile Blog*, February 2, 2012. As of July 7, 2016: http://googlemobile.blogspot.com/2012/02/android-and-security.html

Madden, Mary, and Lee Rainie, *Americans' Views About Data Collection and Security*, Pew Research Center, May 20, 2015. As of November 17, 2015: http://www.pewinternet.org/2015/05/20/americans-views-about-data-collection-and-security/

McDaniel, Patrick, "Bloatware Comes to the Smartphone," *IEEE Security and Privacy*, Vol. 10, No. 4, July–August 2012, pp. 85–87.

Microsoft, "Security Considerations for Reflection," *Microsoft Developer Network*, 2016. As of February 17, 2016: https://msdn.microsoft.com/en-us/library/stfy7tfc(v=vs.110).aspx

Miller, Charlie, "Real World Fuzzing," *Independent Security Evaluators*, October 19, 2007. As of May 24, 2016: https://crypto.stanford.edu/cs155/papers/fuzzing.pdf

Muslukhov, Ildar, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov, "Understanding Users' Requirements for Data Protection in Smartphones," *2012 IEEE 28th Technical Conference on Data Engineering Workshops*, April 1–5, 2012, pp. 228–235. As of July 7, 2016: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6313685

OECD Publishing, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Organisation for Economic Co-operation and Development, 2002. As of July 7, 2016: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

State of California Department of Justice, Office of the Attorney General, "Press Release: Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit," Sacramento, Calif., July 19, 2012a. As of June 2, 2016: http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection

———, "Press Release: Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law," Sacramento, Calif., October 30, 2012b. As of June 2, 2016: http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance

Taylor, Linnet, "No Place to Hide? The Ethics and Analytics of Tracking Mobility Using Mobile Phone Data," *Environment and Planning D: Society and Space*, Vol. 34, No. 2, 2015, pp. 319-336, DOI: 0263775815608851.

Turnow, Joseph, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*, New Haven, Conn.: Yale University Press, 2012.

نبذة عن المؤلفين

جمع باحثون من مؤسسة RAND ومختبر لينكولن التابع لمعهد ماساتشوستس للتكنولوجيا خبراتهما في مجال التكنولوجيا والسياسات والقانون للحصول على فهم أوسع لقضايا خصوصية الهاتف الذكي.

أعضاء فريق RAND

ريبيكا باليباكو (Rebecca Balebako): عالمة كمبيوتر تركز أبحاثها على الخصوصية الرقمية والتفاعل بين الإنسان والحاسوب.

آن بوستيد (Anne Boustead): تعمل على تحضير رسالة الدكتوراه في تحليل السياسات ومحامية تدرس القضايا المتعلقة بالخصوصية والتكنولوجيا والتباين في قوانين الدول.

كارلين ستانلي (Karlyn Stanley): محامية متخصصة في التقنيات الناشئة وتملك خبرة واسعة في تمثيل شركات الاتصالات المحمولة وشركات البنية التحتية اللاسلكية (الأبراج الخلوية)، وعملاء آخرين في مجال الاتصالات بمن فيهم شركة "آي تي إن تي" (AT&T).

ويليام (بيل) ويلسر الرابع (William (Bill) Welser IV): مدير قسم الهندسة والعلوم التطبيقية في RAND. تشمل خبرته البحثية التشفير التطبيقي وسياسة التكنولوجيا.

زيف وينكلمان (Zev Winkelman): مهندس كمبيوتر ويحمل شهادة دكتوراه في السياسة العامة والبحوث، ويركز على قضايا الخصوصية والأمن.

أعضاء فريق مختبر لينكولن التابع لمعهد ماساتشوستس للتكنولوجيا

أركادي يروخيموفيتش (Arkady Yerukhimovich): موظف تقني في مختبر لينكولن، ويحمل خبرة بحثية في التشفير النظري والعملي. ركزت أبحاثه الأخيرة على الاستفادة من أدوات التشفير النظرية لحماية الخصوصية والأمن في التطبيقات على أرض الواقع.

روب كنينغهام (Rob Cunningham): قائد مجموعة النظم والتكنولوجيا الآمنة والمرنة (Secure, Resilient Systems and Technology Group) في مختبر لينكولن. يملك خبرة بحثية واسعة تغطي التعلم الآلي ومعالجة الصور وأمن الكمبيوتر. كما أنه يهتم بمجال الشؤون المتصلة بتكنولوجيات الحفاظ على الخصوصية.

ريك هوسلي (Rick Housley): طالب في هندسة الكمبيوتر يسعى للحصول على درجة البكالوريوس والماجستير في معهد ستيفنز للتكنولوجيا (Stevens Institute of Technology). يركز عمله إلى حد كبير على النماذج المدمجة في الأجهزة والأمن المدمج في الأجهزة.

ريتشارد شاي (Richard Shay): موظف فني في مختبر لينكولن. يملك خبرة بحثية في مجال قابلية استخدام الخصوصية والأمان.

تشاد سبنسكي (Chad Spensky): باحث في مجال الكمبيوتر وعضو في سيكلاب (SecLab) في جامعة كاليفورنيا، سانتا باربرا، ومجموعة "سايبر سيستيم أسيسمنتس" (Cyber System Assessments) في مختبر لينكولن. تشمل اهتماماته البحثية الحالية بروتوكولات الأمن منخفضة المستوى على منصات الهواتف المحمولة، والأمن المدمج في الأنظمة، وأمن البطاقات الذكية، والمصادقة العملية، وتقنيات الفحص الذاتي الجديدة.

جيفري ستيوارت (Jeffrey Stewart): زميل مشارك في مجموعة تقييم النظام الإلكتروني (Cyber System Assessments) في مختبر لينكولن. يملك خبرة في مجال الأنظمة المدمجة وأمن النظام منخفض المستوى.

آري تراختنبرغ (Ari Trachtenberg): أستاذ الهندسة الكهربائية والكمبيوتر في جامعة بوسطن. شارك في المشروع بينما كان منتدبًا إلى مختبر لينكولن.

عن هذا التقرير

يوثق هذا التقرير نتائج البحوث التي نتجت عن التعاون بين مختبر لينكولن (Lincoln Laboratory) التابع لمعهد ماساتشوستس للتكنولوجيا (MIT) ومؤسسة RAND. حمل مشروع RAND عنوان "نظرة عامة على التشريعات المتعلقة بحماية خصوصية بيانات مستخدمي الأجهزة المحمولة"، في حين حمل مشروع مختبر لينكولن عنوان "خصوصية المستخدم على أجهزة آي أو إس وأندرويد". وقد رعى برنامج براندیز (Brandeis Program) ضمن مكتب الابتكار المعلوماتي (Information Innovation Office) التابع لوكالة المشاريع البحثية الدفاعية المتقدمة (Defense Advanced Research Projects Agency) هذا العمل.

يقدم هذا التقرير تقييمًا لخصوصية مستخدمي الهواتف الذكية من المنظورين التقني والتنظيمي. من المنظور التقني، يصف التقرير مراجعة الدراسات والتجارب التي أجراها مختبر لينكولن للتحقيق في حالة الخصوصية على منصات الهواتف الذكية الرئيسية الحالية في عام 2015: نظام التشغيل أندرويد التابع لشركة جوجل ونظام آي أو إس التابع لشركة أبل. أما من المنظور التنظيمي، فيصف هذا التقرير الآليات التنظيمية الفدرالية الرئيسية لحماية الخصوصية في الولايات المتحدة، ويقدم إطارًا لتحديد الثغرات ونقاط القوة في حماية الخصوصية من المنظورين التقني والتنظيمي.

رعت وكالة مشاريع الأبحاث المتطوّرة الدفاعيّة (DARPA) جزء الدراسة الخاص بمؤسسة RAND والذي أُجري في مركز سياسات الاستحواذ والتكنولوجيا التابع لمعهد أبحاث RAND للدفاع الوطني، وهو مركز بحوث وتطوير يعمل بتمويل فدرالي وبرعاية مكتب وزير الدفاع وهيئة الأركان المشتركة وقيادة المقاتلين الموحّدة وقوّات البحرية وقوّات مشاة البحريّة ووكالات الدفاع ومجموعة استخبارات الدفاع.

لمزيد من المعلومات حول مركز سياسات الاستحواذ والتكنولوجيا التابع لمؤسسة RAND، يرجى زيارة www.rand.org/nsrd/ndri/centers/atp أو الاتصال بالمدير (تتوفر معلومات الاتصال على صفحة الويب).

يستند جزء مختبر لينكولن التابع لمعهد ماساتشوستس للتكنولوجيا في هذا البحث إلى العمل الذي تدعمه وكالة المشاريع البحثية الدفاعية المتقدمة بموجب عقد القوات الجوية رقم FA8721-05-C-0002 و/أو FA8702-15-D-0001. إن أي آراء أو نتائج أو استنتاجات أو توصيات معبر عنها في هذه المادة هي آراء المؤلف أو المؤلفين ولا تعكس بالضرورة وجهات نظر وكالة مشاريع الأبحاث المتطورة الدفاعية.

حقوق الطبع والنشر الإلكتروني محدودة

هذه الوثيقة والعلامة (العلامات) التجارية الواردة فيها محمية بموجب القانون. يتوفر هذا التمثيل للملكية الفكرية الخاصة بمؤسسة RAND للاستخدام لأغراض غير تجارية حصريًا. يحظر النشر غير المصرح به لهذا المنشور عبر الإنترنت. يصرح بنسخ هذه الوثيقة للاستخدام الشخصي فقط، شريطة أن تظل مكتملة دون إجراء أي تعديل عليها. يلزم الحصول على تصريح من مؤسسة RAND لإعادة إنتاج أو إعادة استخدام أي من الوثائق البحثية الخاصة بنا، بأي شكل كان، لأغراض تجارية. للمزيد من المعلومات حول إعادة الطباعة والتصاريح ذات الصلة، الرجاء زيارة صفحة التصاريح في موقعنا الإلكتروني: www.rand.org/pubs/permissions.html.

للحصول على مزيد من المعلومات حول هذا المنشور، يرجى زيارة الموقع الإلكتروني التالي: www.rand.org/t/rr1393.

© حقوق الطبع والنشر لعام 2016 محفوظة لصالح مؤسسة RAND

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

مختبر لينكولن التابع لمعهد ماساتشوستس للتكنولوجيا هو مركز بحوث وتطوير يعمل بتمويل فدرالي وبرعاية مكتب وزير الدفاع ويعمل على حل المشكلات التي تمس الأمن القومي.

مؤسسة RAND مؤسسة بحثية تعدّ حلولاً لتحديات السياسات العامة للمساهمة في جعل المجتمعات من حول العالم أكثر أمانًا، سلامة، صحة وازدهارًا. تعدّ مؤسسة RAND مؤسسة غير ربحية، حيادية وملتزمة بالصالح العام.

RAND CORPORATION

لا تعكس منشورات مؤسسة RAND بالضرورة آراء عملاء ورعاة الأبحاث الذين يتعاملون معها. RAND® علامة تجارية مسجلة.

www.rand.org

Arabic Translation
"Can Smartphones and Privacy Coexist"
RR-1393/1-DARPA