Assessing Mobile App Data Privacy Risk

iapp kryptowire

Assessing Mobile App Data Privacy Risk

Executive Summary

By some estimates, more than six billion smartphones will be in use worldwide by 2020. These pocket-sized computers now serve as a platform for a vast ecosystem of applications that provide entertainment, commerce, navigation, professional assistance, even services that improve fitness, health and quality of life.

However, mobile apps and connected devices also generate and collect vast quantities of data about the devices, their uses, and their users. Much of this data is personal and some is quite sensitive. The app-driven data economy thus presents risks for mobile app developers and businesses as well as new challenges for privacy professionals globally. Privacy pros must balance their companies' business needs against consumer privacy concerns and compliance obligations — and do so against a backdrop of their organization's risk tolerance.

Each organization performs this calculus in something of a vacuum. Just how risky is it to collect and process precise geolocation data in real time? How does that compare against enabling a mobile device's microphone or camera? Is it advisable to ask for users' credit card information or bank account details? And how about aggregating a user's fitness training and sleeping patterns over time? In many cases, the risk assessment depends on multiple factors, including the nature of the data collected, the service offered, consumer transparency, and choice.

However, it would clearly be useful to have a baseline for assessing app data privacy risk. To that end, the IAPP asked approximately 400 privacy professionals to rate their perception of risk associated with a variety of data collected and used via mobile apps. Our aim was to determine, from the perspective of an enterprise deploying a mobile app, the degree of risk the enterprise is exposed to as a result of collecting and using certain consumer- or device-related data. To be sure, this risk assessment does not necessarily reflect consumer perception of risk created by collection and use of the same data. But the risk measured by privacy professionals who deal with data collection and use day in, day out, is clearly meaningful.

Privacy pros must balance their companies' business needs against consumer privacy concerns and compliance obligations — and do so against a backdrop of their organization's risk tolerance.

We found that the highest risk score is assigned to information that presents security vulnerability and can be misused for theft or fraud, such as passwords and credit card or banking information. Information traditionally considered "sensitive," like health and children's information, not surprisingly, also ranks high.

Privacy professionals also raise concerns about data collection and use that can be perceived as "creepy": for example, activating a device's camera or microphone, viewing text messages, or accessing video or audio recordings. Much of this information is uniquely associated with mobile apps because they are deployed on devices that travel everywhere with a user and may serve multiple personal and business needs.

The privacy of users' browser history is currently a hot privacy topic in the United States, where Congress recently eliminated requirements that internet service providers get consumer consent before using browsing history for advertising and marketing. Interestingly, browser history did not make the top-tier of risk concerns among survey respondents, nor did users' geolocation, always a hotly debated issue in privacy circles. Also low on the scale is the privacy of persistent identifiers like device ID, or information about other connected devices, which attract a great deal of attention among policymakers and industry groups.

Privacy professionals also raise concerns about data collection and use that can be perceived as "creepy": for example, activating a device's camera or microphone, viewing text messages, or accessing video or audio recordings.

This report ranks mobile app data risks globally and compares the results from respondents in the U.S. and the European Union, where cultural and legal differences drive some interesting variations in perceptions of mobile app privacy risks. For instance, European respondents overall tend to assign higher risk scores than their American counterparts. EU respondents are significantly more likely to assign high risk scores to biometric information, to data that reveals a user's personal connections like phone and text logs and remote numbers called, and to social networking connections. Privacy professionals from the EU also rate as considerably more risky the use of data collected through mobile apps for third-party advertising, predictive analytics for marketing, and cross-device tracking.

Research Methods

In February 2017, the IAPP fielded an anonymous online survey to subscribers of the IAPP's Daily Dashboard, yielding around 400 total survey responses from around the globe. We asked respondents to assume their enterprise is developing or deploying a mobile application and to rate the risk to their organization based on the type of data collected or the uses of collected data. We defined "risk" as the potential for liability, regulatory non-compliance, or even harm to the company's brand.

For each data type or use, respondents were given the choice of "very low risk," "low risk," "moderate risk," "elevated risk," or "high risk." They were also given the option to check "don't know" for each question.

In this report, we present the results for each data risk category in two ways: (1) by mean score on a scale of one to five; and (2) by an overall risk score displayed as a percentage and ranked based upon how many responses scored either a four or a five ("elevated" or "high" risk). In both cases we filtered out the "don't know" answers.

Respondents' Demographics

More than 50 percent of responses came from U.S.-based privacy professionals, with 23 percent from the European Union including the United Kingdom. Because the number of responses from other regions of the world was not statistically robust, we did not break out those regional responses for comparison, but they are included in the aggregate totals.

The Software and Services industry is best represented in this survey with 15.87 percent of the respondents, followed by the Government sector at 11.34 percent.

Country Distribution

United States	238	53.97%
European Union (including the U.K.)	103	23.35%
Canada	54	12.24%
Asia	17	3.85%
Non-EU Europe	10	2.27%
Latin America (including Mexico)	5	1.13%
Australia	7	1.59%
Africa	2	0.45%
Middle East	2	0.45%

Industry Distribution

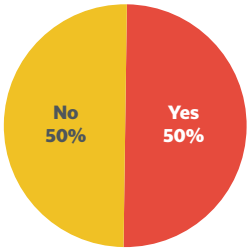
Aerospace and Defense	0.91%	Hotels, Restaurants and Leisure	1.36%
Banking	5.67%	Household and Personal Products	0.91%
Business Services and Supplies	8.84%	Insurance	7.26%
Capital Goods	0.23%	Materials	0.00%
Chemicals	0.45%	Media	3.40%
Conglomerates (multiple sectors)	1.13%	Nonprofit	7.03%
Construction	0.00%	Oil and Gas Operations	0.45%
Consumer Durables	0.23%	Retailing	3.85%
Diversified Financials	2.04%	Semiconductors	0.91%
Drugs and Biotechnology	2.95%	Software and Services	15.87%
Education and Academia	5.90%	Technology Hardware and Equipment	2.49%
Food, Drink or Tobacco	0.68%	Telecommunication Services	4.31%
Food Markets	0.00%	Trading Companies	0.45%
Government	11.34%	Transportation	1.36%
Healthcare Equipment and Services	8.84%	Utilities	1.13%

The most common positions held by privacy pros who responded to the survey are manager-level positions at 19.50 percent, followed closely by directors at 18.14 percent, after which the next most common role is the assistant or associate counsel at 11.56 percent. Privacy program leads and those who are not leads are represented equally.

Title Distribution

Manager level	19.50%
Director level (not Board)	18.14%
Assistant or Associate Counsel level	11.56%
C-Suite level	7.48%
Lead Counsel level	7.48%
Individual Contributor	7.26%
Vice President level	5.67%
Analyst	5.22%
Solutions Architect	2.49%
Senior Vice President level	2.27%
Coordinator	2.04%
Executive Vice President level	1.13%
Supervisor	0.91%
Other	8.84%

Are you the privacy lead for your company?



Data Collected by Mobile Applications

Mobile applications are exploding as companies look for new ways to provide services to their customers, interact with them, and gather valuable business data in the process. Some companies exist entirely to develop and deploy applications in the mobile environment. Others are in the business of selling products or services but are developing apps to enhance their customers' experiences and support them in innovative ways.

One such company is Nike, Inc., and Nike's Marilyn Prosch in some ways represents a new type of privacy professional. Nike is primarily in the business of selling shoes and clothing, but Prosch's title at Nike is privacy manager-mobile, reflecting her role working directly and exclusively with programmers developing the company's mobile apps. She is embedded with the app team to address privacy before anyone writes a single line of code. She's even growing her team to keep up with the demand for Nike's mobile offerings – and the significant quantity of data and privacy issues presented by mobile apps.

Mobile apps present new privacy risks because they are downloaded to a personal device where many users store considerably more personal information than they would on a desktop or laptop. They can also present more complicated compliance issues: Providing meaningful notice on a tiny screen is challenging. As apps are deployed globally, moreover, privacy professionals struggle with issues involving privacy regulations that differ across jurisdictional borders and with users who have disparate cultural norms and multiple languages.

Jill Bronfman, who studies cross-cultural privacy issues and emerging technologies as an affiliate scholar with Hastings

Law School and is of counsel with Sycamore Legal, offered a reminder not to limit the definition of mobile apps to software downloaded to phones: "Mobile devices include vehicles, toys, drones, and other connected things. They are not separate categories from a privacy perspective."

Privacy laws and practices must converge, Bronfman said, because "at some point almost everything will be connected to the internet and will be a mobile device. The idea of having separate privacy and security standards for each of these things will fall away, and we will need to analyze privacy from what personal data is collected and how it's used, rather than what device it's from."

Our research reflects how privacy professionals rate privacy risk from a liability and compliance perspective, but it could also be viewed as a consumer privacy sensitivity score. Not surprisingly, our research shows that privacy professionals consider regulated information like medical information, bank information, or children's information, or information covered by data breach laws like credit card information, to be among the most risky to the enterprise. They also rate as "high risk" information that is highly personal, such as email or messaging content, live images from a camera, live audio from a microphone, or passwords.

Evan apart from regulated and other "sensitive" information, risk abounds with actions mobile apps might take on the device that a consumer might not expect. It might surprise a consumer, for instance, if a mobile app could track the user's location, gain access to other accounts on the device, or view the user's contact list. These actions present risks, then, not only of enforcement actions by regulators but also of lost consumer trust.

As discussed above, we present the data in multiple ways. We provide two tiers of risk assessment cutting across data collected and data uses, basing our ranking on the mean numeric score earned by each category on a 5-point scale after removing the "don't know" responses. In addition, we break out the percentage of responses for each risk level (low to high) and rank the responses by adding the "elevated" (4) and "high" (5) scores together. We then create color-coded "risk zones" depending on how each category scored using the percentage method. There are four risk zones for the "collected data" categories and two for the "data uses" categories.

Top 10 Privacy Risks for Mobile App Developers (Mean Score, Scale 1-5):

1	Collecting passwords	4.63
2	Collecting credit card number	4.59
3	Collecting disease status	4.59
4	Collecting disease symptoms	4.59
5	Producing medical diagnosis	4.58
6	Collecting bank information	4.57
7	Collecting children's information	4.56
8	Collecting live imagery	4.49
9	Collecting email content	4.48
10	Activating camera	4.41

Red zone: highest risk
Orange zone: elevated risk
Blue zone: moderate risk
Green zone: lowest risk

Mobile App Risks Zones: Data Collected

		Risk					
Data	Mean Score	Very Low (1)	Low (2)	Moderate (3)	Elevated (4)	High (5)	Risk Score (4+5)
Credit card number	4.59	1.50%	0.50%	5.25%	23.25%	69.50%	92.75%
Bank information	4.57	1.50%	0.50%	5.51%	24.56%	67.92%	92.48%
Children's information	4.56	1.25%	2.25%	5%	22.50%	69.00%	91.5%
Disease status	4.59	1.26%	2.02%	5.29%	19.40%	72.04%	91.44%
Passwords	4.63	0.75%	1.75%	6.27%	16.04%	75.19%	91.23%
Camera: live imagery	4.49	0.77%	2.05%	7.95%	25.64%	63.59%	89.23%
Email content	4.48	0.25%	1.77%	9.37%	27.34%	61.27%	88.61%
Microphone: live audio	4.40	1.03%	3.59%	9.74%	25.64%	60.00%	85.64%
Disease symptoms	4.38	1.76%	4.28%	9.07%	24.94%	60.20%	85.14%
SMS or MMS content	4.32	1.53%	2.80%	13.23%	27.48%	54.96%	84.44%
Medication compliance	4.33	2.02%	3.03%	10.86%	27.78%	56.31%	84.09%
Recorded video or photos	4.30	0.77%	3.32%	12.02%	33.25%	50.64%	83.89%
Recorded audio	4.28	1.02%	2.81%	13.30%	33.25%	49.62%	82.87%
Transaction data	4.24	1.52%	2.27%	15.15%	32.32%	48.74%	81.06%
Access to other accounts	4.18	1.03%	3.35%	16.24%	35.57%	43.81%	78.38%

Red zone: highest risk
Orange zone: elevated risk
Blue zone: moderate risk
Green zone: lowest risk

Mobile App Risks Zones: Data Collected

		Risk					
Data	Mean Score	Very Low (1)	Low (2)	Moderate (3)	Elevated (4)	High (5)	Risk Score (4+5)
Phone and text logs	4.05	0.76%	3.80%	19.75%	41.01%	34.68%	75.69%
Biometrics (heart rate, sleep patterns, stress)	4.08	2.54%	8.88%	14.21%	26.40%	47.97%	74.37%
Location tracking	3.93	3.76%	6.80%	18.78%	33.57%	37.09%	70.66%
Contacts' personal information	3.93	1%	5.30%	25.51%	35.86%	32.32%	68.18%

Red zone: highest risk
Orange zone: elevated risk
Blue zone: moderate risk
Green zone: lowest risk

Mobile App Risks Zones: Data Collected

		Risk					
Data	Mean Score	Very Low (1)	Low (2)	Moderate (3)	Elevated (4)	High (5)	Risk Score (4+5)
Remote number connected by call	**3.68**	1.91%	7.65%	31.97%	**37.70%**	20.77%	58.47%
Calendar information	**3.69**	1.28%	8.97%	**32.82%**	**32.82%**	24.10%	56.92%
Location tags on pictures	**3.50**	5.44%	10.64%	31.44%	**33.10%**	19.39%	52.59%
Browser history	**3.48**	2.82%	13.18%	**34.12%**	33.41%	16.47%	49.88%
Current location	**3.42**	6.64%	13.50%	**31.80%**	27.49%	20.62%	48.11%
Frequency of contact (# of texts, calls, etc.)	**3.40**	3.53%	16.12%	**32.75%**	32.24%	15.37%	47.61%
Social networking connections	**3.43**	2.27%	13.39%	**38.13%**	31.31%	14.90%	46.21%
Device ID	**3.36**	3.33%	16.67%	**36.15%**	28.21%	15.64%	43.85%
Names of other Wi-Fi connected devices	**3.31**	6.24%	17.51%	**32.61%**	25.90%	17.75%	43.65%
Which other apps are running	**3.18**	5.47%	19.52%	**37.62%**	25.95%	11.43%	37.38%
Connected devices	**3.19**	3.63%	22.86%	**36.88%**	24.42%	12.21%	36.63%

Red zone: highest risk
Orange zone: elevated risk
Blue zone: moderate risk
Green zone: lowest risk

Mobile App Risks Zones: Data Collected

		Risk					
Data	Mean Score	Very Low (1)	Low (2)	Moderate (3)	Elevated (4)	High (5)	Risk Score (4+5)
Frequency/duration of exercise	3.10	6.35%	24.11%	35.03%	21.83%	12.69%	34.52%
Bookmarked pages	3.10	5.25%	23.15%	37.47%	24.58%	9.55%	34.13%
Education data	3.08	7.12%	23.92%	35.62%	20.10%	12.23%	32.33%
Wi-Fi connection status	2.65	16.35%	33.65%	26.68%	15.87%	7.45%	23.32%
Internet connectivity	2.74	11.89%	33.33%	32.04%	14.73%	8.01%	22.74%
Call duration	2.73	8.33%	37.12%	33.33%	15.57%	5.56%	21.13%

Red zone: highest risk
Orange zone: elevated risk
Blue zone: moderate risk
Green zone: lowest risk

Mobile App Risks Zones: Data Uses

Data	Mean Score	Risk: Very Low (1)	Low (2)	Moderate (3)	Elevated (4)	High (5)	Risk Score (4+5)
Producing medical diagnosis	**4.58**	1.08%	1.36%	8.13%	17.07%	**72.36%**	89.43%
Storing data in plain text	**4.42**	1.08%	1.88%	9.41%	28.76%	**58.87%**	87.63%
Activating camera	**4.41**	1.10%	2.21%	9.94%	27.62%	**59.12%**	86.74%
Activating microphone	**4.36**	1.38%	3.04%	14.64%	23.20%	**58.29%**	81.79%
Allowing all-ages use without requiring parental consent	**4.27**	2.22%	3.05%	15.24%	23.82%	**55.68%**	79.50%
Identifying a home address	**4.15**	0.82%	3.28%	18.58%	34.43%	**42.90%**	77.33%
Preventing device screen lock	**4.17**	1.93%	7.71%	14.33%	23.97%	**52.07%**	76.04%

Red zone: highest risk
Orange zone: elevated risk
Blue zone: moderate risk
Green zone: lowest risk

Mobile App Risks Zones: Data Uses

		Risk					
Data	Mean Score	Very Low (1)	Low (2)	Moderate (3)	Elevated (4)	High (5)	Risk Score (4+5)
Lack of just-in-time privacy notice	**3.79**	1.95%	6.96%	27.86%	**36.49%**	26.74%	63.23%
Linking accounts across platforms	**3.79**	1.89%	7.55%	28.57%	**33.69%**	28.30%	61.99%
Complex privacy notice	**3.58**	4.38%	11.23%	27.95%	**34.79%**	21.64%	56.43%
Defaulting to opt-out consent	**3.44**	12.33%	9.86%	23.84%	**29.04%**	24.93%	53.97%
Storing data on the device	**3.51**	3.49%	14.78%	27.96%	**34.95%**	18.82%	53.77%
Cross-application advertising	**3.52**	2.47%	13.19%	32.14%	**34.62%**	17.58%	52.20%
Creating a user account	**3.47**	4.90%	17.44%	**26.98%**	26.70%	23.98%	50.68%
Predictive analytics for marketing	**3.27**	2.63%	16.58%	35.00%	**36.84%**	13.16%	50.00%
Condition-targeting for advertising	**3.44**	3.44%	14.04%	**33.81%**	32.38%	16.33%	48.71%
Serving third-party advertising	**3.73**	4.12%	15.53%	**32.15%**	31.61%	16.62%	48.23%
Drawing screens or pop-over windows on app	**3.35**	2.05%	19.88%	**33.04%**	30.99%	14.04%	45.03%
Look-alike modeling for advertising	**3.29**	3.23%	19.41%	**34.41%**	30.59%	12.35%	42.94%

Geography matters

As privacy professionals know, privacy laws and practices differ across the globe, along with consumer attitudes and data sharing habits. The EU's new General Data Protection Regulation (GDPR) takes a risk-based approach to privacy regulation, focusing on protecting the fundamental rights and freedoms of data subjects and adopting a broad definition of personal data. Data processing activities considered a "high risk" trigger heightened obligations under the GPDR, including a duty to prepare a Data Protection Impact Assessment and perhaps consult with a Data Protection Authority, and enhanced data breach notification responsibilities. In the U.S., by contrast, personal information is regulated by sector or type of personal information (e.g. health, financial, or children's information), by how it is collected (e.g. by drones or online), and by state data breach laws.

In her research, Bronfman has observed that family and ancestry can be sensitive subjects in Asia, and EU citizens may be reluctant to disclose their union membership status or religious affiliations. These subjects are often discussed openly in the U.S. At Nike, Prosch and her privacy team help mobile app programmers consider global privacy sensibilities when deciding what data to integrate into their sports-related apps – what works for the U.S. market might not be acceptable elsewhere.

Julie Jacobson, a K&L Gates attorney who works with companies worldwide, finds EU-based clients are the most likely to have an in-house privacy officer and be well on their way to complying with the GDPR, which takes effect in May 2018. Her U.S.-based clients fall on a spectrum, however. Larger or regulated companies tend to be the most privacy sensitive with their mobile apps and the most willing to accept a broad definition of personal information, while smaller companies – especially start-ups devoted exclusively to mobile-app development – tend to be the least privacy savvy.

"Non-U.S. companies are more privacy sensitive from the start," Jacobson observed. "They start with a higher level of privacy awareness because no matter what industry they're in they are subject to privacy regulation."

In Jacobson's experience, the thorniest issues for her U.S. clients involve health-related apps, integrating text messaging into telemarketing campaigns, mobile banking, and anything involving cross-border data transfer. Otherwise, she said, in the U.S., if you're not covered by federal health or financial data protection laws, "you're just looking at California law."

California's Online Privacy Protection Act defines "personal information" relatively broadly to include an "identifier that permits the physical or online contacting of a specific individual," as well as "information concerning a user [collected] online from the user and [maintained] in personally identifiable form in combination with" another identifier. California and the Federal Trade Commission have both published guidelines and recommendations for mobile privacy practices.

Because of the small sample size from Canada, Asia, and other parts of the world, we limited our comparative analysis to responses from U.S.-versus EU-based privacy professionals. On balance, the two regions tend to put the same data categories in the same risk "zones." The EU privacy professionals on balance give higher numeric risks scores to all data categories across the board, likely owing to their different view of privacy risk, but perhaps as well to the smaller sample size, which in this study tended to make mean scores higher.

Where we see statistically meaningful differences among collected data categories are in areas like user's social connections, where the EU respondents give phone and text logs, remote numbers called, and social networking connections

a significantly higher risk rating than their U.S. counterparts do. EU respondents are also far more concerned about the names of other Wi-Fi connected devices than those in the U.S., for whom that was quite low on the risk register.

We also see meaningful risk distinctions among EU and U.S. respondents for actions relating to notification and consent, where there's some possibility of data subjects not being unambiguously informed, as well as using personal data for advertising. For example, the EU respondents give significantly higher risk scores for "providing just-in-time privacy notice," having a "complex privacy policy," and "defaulting to opt-out consent," signals of hot spots for U.S. companies preparing for GDPR compliance next year. Europeans assigned a higher risk score by more than 20 percentage points for "cross application advertising," "condition-targeting for advertising," and "look-alike modeling for advertising."

Data Collected	U.S.	EU	Data Collected	U.S.	EU
Credit card number	92.20%	97.78%	Contacts' personal information	65.58%	68.09%
Bank information	94.01%	86.67%	Remote number connected by call	54.08%	65.85%
Children's information	91.28%	91.11%	Calendar information	49.52%	67.04%
Disease status	91.20%	91.02%	Location tags on pictures	48.90%	56.56%
Passwords	89.86%	93.34%	Browser history	45.61%	53.53%
Camera: live imagery	87.20%	91.01%	Current location	46.02%	50.01%
Email content	85.45%	92.22%	Frequency of contact (# of texts, calls, etc.)	43.25%	52.22%
Microphone: live audio	82.94%	89.89%	Social networking connections	41.32%	55.56%
Disease symptoms	84.72%	88.77%	Device ID	38.68%	51.14%
SMS or MMS content	79.25%	86.67%	Names of other Wi-Fi connected devices	38.63%	59.00%
Medication compliance	84.65%	89.89%	Which other apps are running	33.64%	42.42%
Recorded video or photos	80.19%	89.89%	Connected devices	31.88%	44.31%
Recorded audio	80.19%	84.27%	Frequency/duration of exercise	32.87%	39.32%
Transaction data	78.89%	81.12%	Bookmarked pages	30.67%	39.79%
Access to other accounts	79.53%	77.27%	Education data	35.38%	25.84%
Phone and text logs	71.36%	81.11%	Wi-Fi connection status	18.55%	32.00%
Biometrics (heart rate, sleep patterns, stress)	72.77%	84.27%	Internet connectivity	20.47%	29.37%
Location tracking	69.30%	74.74%	Call duration	19.71%	22.23%

U.S. Top 10 Data Collection Risks

Rank	Data collected	Risk score	Mean score
1	Bank information	94.01%	4.64
2	Credit card number	92.20%	4.59
3	Children's information	91.28%	4.59
4	Disease status	91.20%	4.58
5	Passwords	89.86%	4.59
6	Camera: live imagery	87.20%	4.41
7	Email content	85.45%	4.42
8	Disease symptoms	84.72%	4.38
9	Medication compliance	84.65%	4.34
10	Microphone: live audio	82.94%	4.34

EU Top 10 Data Collection Risks

Rank	Data collected	Risk score	Mean score
1	Credit card number	97.78%	4.49
2	Passwords	93.34%	4.67
3	Disease status	91.02%	4.67
4	Disease symptoms	88.77%	4.55
5	Email content	92.22%	4.53
6	Children's information	91.11%	4.50
7	Camera: live imagery	91.01%	4.54
8	Medication compliance	89.89%	4.51
9	Recorded video or photos	89.89%	4.40
10	Microphone: live audio	89.89%	4.44

U.S. Top 5 Data Use Risks

Rank	Data used	Risk score	Mean score
1	Producing medical diagnosis	87.82%	4.56
2	Storing data in plain text	88.50%	4.46
3	Activating camera	86.01%	4.39
4	Allowing all-ages use without requiring parental consent	80.31%	4.32
5	Activating microphone	78.76%	4.29

EU Top 5 Data Use Risks

Rank	Data used	Risk score	Mean score
1	Producing medical diagnosis	87.95%	4.61
2	Activating camera	87.81%	4.45
3	Storing data in plain text	87.21%	4.40
4	Activating microphone	84.34%	4.39
5	Identifying a home address	80.72%	4.19

Significant Differences: Comparing U.S. vs EU Risk Scores for Data Collected

	Location	(1)	(2)	(3)	(4)	(5)	(4+5)
Phone and text logs	**U.S.**	0.93%	5.63%	22.07%	**37.56%**	33.80%	71.36%
	EU	1.11%	0.00%	17.78%	**50.00%**	31.11%	81.11%
Biometrics (heart rate, sleep patterns, stress)	**U.S.**	2.82%	9.86%	14.55%	26.76%	**46.01%**	72.77%
	EU	3.37%	4.49%	7.87%	24.72%	**59.55%**	84.27%
Remote number connected by call	**U.S.**	3.06%	9.69%	33.16%	**33.67%**	20.41%	54.08%
	EU	1.22%	4.88%	28.05%	**45.12%**	20.73%	65.85%
Social networking connections	**U.S.**	3.29%	16.90%	**38.97%**	27.70%	13.62%	41.32%
	EU	1.11%	8.89%	34.44%	**40.00%**	15.56%	55.56%
Names of other Wi-Fi connected devices	**U.S.**	5.91%	19.09%	**36.82%**	23.18%	15.45%	38.63%
	EU	5.00%	12.00%	24.00%	**35.00%**	24.00%	59.00%
Wi-Fi connection status	**U.S.**	16.74%	**39.37%**	25.34%	11.76%	6.79%	18.55%
	EU	12.00%	20.00%	**36.00%**	24.00%	8.00%	32.00%

Significant Differences: Comparing U.S. vs EU Risk Scores for Data Uses

	Location	(1)	(2)	(3)	(4)	(5)	(4+5)
Lack of just-in-time privacy notice	**U.S.**	2.63%	9.47%	28.42%	**34.21%**	25.26%	59.47%
	EU	1.22%	4.88%	21.95%	**36.59%**	35.37%	71.96%
Linking accounts across platforms	**U.S.**	2.02%	8.08%	**32.82%**	30.81%	26.26%	57.07%
	EU	2.30%	5.75%	24.14%	**34.48%**	33.33%	67.81%
Complex privacy notice	**U.S.**	4.66%	13.47%	29.53%	**34.72%**	17.62%	52.34%
	EU	1.19%	11.90%	19.05%	**36.90%**	30.95%	67.85%
Defaulting to opt-out consent	**U.S.**	15.03%	12.44%	25.39%	**28.50%**	18.65%	47.15%
	EU	7.14%	5.95%	19.05%	28.57%	**39.29%**	67.86%
Cross-application advertising	**U.S.**	3.06%	14.29%	**36.73%**	34.69%	11.22%	45.91%
	EU	1.18%	14.12%	17.65%	**37.65%**	29.41%	67.06%
Predictive analytics for marketing	**U.S.**	3.98%	21.39%	**39.80%**	26.87%	7.96%	34.83%
	EU	1.19%	10.71%	26.19%	**36.90%**	25.00%	61.90%
Condition-targeting for advertising	**U.S.**	3.26%	15.76%	**40.22%**	27.71%	13.04%	40.75%
	EU	3.61%	12.05%	21.69%	**39.76%**	22.89%	62.65%
Serving third-party advertising	**U.S.**	4.06%	19.29%	**33.50%**	30.96%	12.18%	43.14%
	EU	3.49%	10.47%	26.74%	**31.40%**	27.91%	59.31%
Look-alike modeling for advertising	**U.S.**	2.81%	24.16%	**37.64%**	26.40%	8.99%	35.39%
	EU	2.47%	16.05%	27.16%	**37.04%**	17.28%	54.32%

Predictions

The GDPR applies to any company doing business with people in the EU. The next major challenges for mobile app developers globally involve building privacy programs to meet the GDPR's broad definition of personal information, explicit consent requirements, and cross border data transfer obligations. The Regulation requires controllers to manage data protection practices according to the risk their data subjects face. These research results help to categorize those risks and inform controllers seeking to invest in privacy practices as to where they should focus their efforts.

Jacobson observes that her U.S. clients are beginning to factor GDPR into their privacy practices and programs. She describes the law as a "sea change" in her clients' approach to privacy, and predicts that the stability of the U.S.-EU. Privacy Shield program is a major focus for many of her clients.

But consumers continue to demand integrated and even immersive products like virtual reality, creating new opportunities for companies along with new privacy challenges. Few consumers will resent the use of health and medical information that might help to save their lives, Bronfman notes, with mobile technologies monitoring and communicating about drug interaction, insulin dosage, pace makers, or even the location and stability of elderly living alone.

Bronfman predicts that technology will be called upon to solve at least some of the privacy problems technology creates. This may include consumer-facing products that help them manage their own data and privacy risks. It will also involve enterprise-level tools that companies will deploy on their employees' mobile devices to guard against apps that might compromise company data stored on or accessible through them.

As mobile apps and connected devices collect and use vast new quantities and categories of data, some of it will inevitably fall into the definition of personal information and present risks to data subjects. Privacy professionals – and the tools they deploy – exist to recognize and mitigate these risks. The proliferation of mobile applications and the Internet of Things therefore inevitably will lead to growth in the privacy profession and the privacy industry.

Conclusion

Privacy risks are not equivalent among data categories or uses, across cultures, or across devices. Mobile app developers need to understand the different privacy risks inherent in collecting certain information, or in unleashing the power to access and use data from apps and tools operating on a mobile device. This report is intended to help guide privacy professionals in assessing privacy risks not just to comply with privacy and data protection laws but also to create privacy-sensitive mobile apps by design.

iapp

Learn More
https://iapp.org/about

kryptowire

Learn More
https://www.kryptowire.com/