Privacy and smartphone apps: What data your phone may be giving away (CBC Marketplace) – Video Transcript

Asha: This is marketplace. Four Canadians, one big surprise.

Hey, Jason.

Hey, how are you?

Asha: They're about to find out we've hijacked their phones. Text messages, we had access to that.

Everything?

We also had access to your camera phone.

What?

Asha: About three quarters of us own a smartphone with a dozen apps or more, but when we download them, how much personal information are we giving up?

I'm in shock. Now I'm just going through my head, what else was I doing on my phone? It makes you feel violated.

Asha: We're putting your privacy to the test like never before. We're creating our very own app. So that's our home page. Using similar privacy policies to popular ones already out there.

How many apps do you have on both those phones?

Too many to count. I guess.

Asha: Why?

Well, it seems like we're getting a lot from them, right? Convenience, entertainment, connecting with friends.

Could you live without apps?

I could, but I'd rather not.

Asha: But what are the consequences? To find out, we're in the tech capital of the world, San Francisco, to meet up with Domingo Guerra, president and co-founder of Appthority.

A lot of times we'll download an app thinking it's a flashlight, thinking it's a game, thinking it's a social media app but it's so much more bundled into it.

Asha: He's analyzed over four million applications. Listen up. He's got a message for every phone addict out there.
An app could act as anything. It could turn on the audio to listen into your conversations even if you're not using the phone. Could turn on the front or back camera to take video or pictures. And it's with you all the time so it's really the perfect spy tool.

Asha: That's why Appthority has agreed to design and build our app. It's got to be something fun and free, so we decide on a horoscope. It's easy to create, but could have big consequences for you.

In less than a day, check this out. A new company and a website complete with an app you can download, called My Daily Horoscope.

Time to make our sales pitch in Toronto.

Our app that we're testing out is called My Daily Horoscope.

Okay.

It's free to download. Are you willing to try it out?

Yeah, sure.

Sure, I could do that.

Asha: Our app is only available to Android phone users. Other platforms won't support it. You're part of an exclusive group that's going to get a sneak peek at our daily horoscope app.

Nice.

Asha: While we get a sneak peek into their lives.

You going to accept?

Of course.

Asha: Remember, our horoscope app has similar permissions as some of the big companies. And everything we have access to is spelled out in our terms and conditions.

Now what?

What's happening there?

You've got to click or read- read those terms and conditions.

You didn't even read them!

I did.

Did you?

My reading skills are -- That was like speed reading.
That was on point.

As a general rule, I know what's going to be in here, but I always like to skim through anyways.

You have to give me a second here.

Asha: Are you reading that quickly?

Skimming. I'm skimming.

Asha: Skimming, okay, okay.

They all agree to our terms before downloading the app, but do they really know what they're giving us access to? Their photos, call logs, text messages, location, even their microphone.

It's an application and user licence agreement.

Ah.

Privacy ones, the ones that no one ever reads.

No one ever reads it?

No.

Asha: Our app expert is not surprised.

It's very difficult to follow up with all the terms and conditions. If we put ourselves in a normal situation, so if you go and buy a shirt at a store and the clerk asks you for your phone number, your parents' phone numbers, your parents' address, your calendar, your location for the last ten days, you'd never do it. But when an app asks for that permission, we have no problem clicking okay.

Asha: Yep, same thing with our testers. But they are eager to read their horoscope.

Kick it...

What's...

You get...

Asha: And just like that, we have instant access to their private lives. Okay. So people have downloaded our app. Let's see what we've got. Let's check out the call logs for one of our testers. Yep, we can see everything. Just a quick scan. And there's some phone calls to mom.

Jason. What have we got here? Sticking out his tongue. Fun selfie. One of the things we can do is record a photo from their actual phone. Let's take a look at this. Go to remote eyes, camera, so we're going to take a picture from the front camera. They have
no clue right now that we're doing this. And let's see if it works. Wow. Yep. That's our tester.

From photos to text messages to call logs, we can even track their location at any moment.

So Shahbaz just popped up here. We're going to find out where he is right now. So there he is. Near a golf club and a fire station. And we have the actual address but we're not going to give you that.

It's pretty unreal that we can see these things on their smartphones. We've only skimmed the surface, but I'm feeling uneasy knowing their personal information is right at my fingertips.

Before our big reveal, I want to know what the real pros can do. We're in Las Vegas about to step into the underground world of hacking. Tag along. This should be interesting. Defcon 24!

Asha: Welcome to Defcon, the largest hacker convention in the world. Where thousands of hackers unite.

This is so cool.

Asha: We're about to meet some white hat hackers. They hack for the greater good to expose flaws in the industry. From the fun and frivolous... So you've created a player that never loses.

Well, why don't we give it a try ourselves here and see how you fare.

Asha: Okay.

I'm getting beat down. I don't even know what I'm doing here.

And there it is.

Asha: Loser.

That's me.

..To hacks with high stakes like this gadget called the Briefcase of Doom. It can clone your credit cards. So you would become me, essentially.

Yes, I would become you until it was no longer financially available because I've already stolen all your money.

Asha: Until you drained all my money out.

Exactly. Then I'm going to be somebody else. And the only thing that you need to do is, it's done.

Asha: Just like that, he can steal my identity. Time to up the ante.
Chris and Michelle are human hackers. No high-tech gadgets here. They say they can hack me using personal info I've shared online.

You're going to assume my identity right now.

Yes, ma'am.

All right. They start by spoofing my number so it looks like they're calling from my phone. After just a few minutes... Um, she just got my balance. Shoot.

Did you just get that?

Yes.

As a recording?

Recording.

She just got my phone balance, what I owe, on a recording. From typing in my phone number, that's it. When she gets a rep on the phone, she stays in character.

Hi, my name is Asha, and I'm hoping you can help me with some account information. And so I just wanted to get the account number, can you -- are you able to give that to me? Oh, that would be so wonderful.

Asha: Now she's digging for my banking details.

Did I use my Visa or Amex on that? Is it just making debit straight from my account then, is that how it's set up? You know what, I'm getting married soon, so I'm wondering if I can get my fiancé added to the account. Thank you. Thank you. We're planning a wedding but it's really stressful, you know.

Asha: It takes no time before this human hacker is able to add someone else to my account. And that's not all.

I'm really super stressed right now, I apologize. Can I do a password reset on the account?

Asha: Whoa, she locks me out. Chris says people share a lot of info about themselves online, making it easy for hackers to find and use against you.

First of all, it's just be cautious of what you put online. Like this is really the crux of it, right?

Asha: So what shouldn't you put online?

Your date of births, your home addresses, your email addresses, we tell people sometimes to have like a throw-away email.

Asha: Word to the wise, lock your information down on the worldwide web.

So how easy is it for the pros to hack into my phone?
It's getting scary. It happens all the time.

Asha: Security researcher Cameron Camp is about to show me just how much I gave away.

You were sent a link.

Asha: Yeah.

And you clicked on that link.

Asha: I did.

And so here's the information that came from that. A picture of you in Hollywood. A fire near your house. And you look wonderful in that wedding dress, and you like taking selfies with your niece. It's easy to know a lot about you from what is on your phone.

Asha: Funny the things that get you. For me, it was seeing a picture of my niece on his computer. And it doesn't stop there. He says he can access my calendar, instant messages, even my banking details. So when it comes to banking, my money could be drained and I wouldn't even know it?

Yes, you would never know.

Asha: After this eye-opening experience, it's time to flip the script. How much information are you giving away?

You guys have access to all my information, you guys could have taken pictures at the wrong time, listen to conversations that were private.

Kind of creepy. It makes you feel violated.

Asha: The big reveal on your marketplace.

Head to our Facebook page for more info.

Asha: How your apps can spy on you, this is your marketplace.

We're on our way to meet up with some smartphone users who have agreed to download our new horoscope app. Using similar permissions as some of the best-known apps out there, we're about to reveal just how much info we're all giving away.

This is the moment of truth.

Hey, Chelsea.

Hi, how are you?

Asha: Great to see you again.

Good to see you again.

About a week ago, we met for the first time.
Yes.
We asked you to download a horoscope app that we created and we talked about the terms and conditions and permissions.
Right, we did talk about that.
Very similar to popular apps like Facebook, Twitter, Snapchat. When you accepted our terms, though, you became a part of a CBC experiment.
Okay.
And you gave up a lot of information. Text messages, we had access to that.
Everything? Oh, my.
You needed a lab coat, did you end up finding one?
Yes, yeah.
You did, hey?
Yeah, I did.
I have no idea what to say.
You gave us permission to look at your call logs. Does this look familiar to you?
It does.
I notice that there's someone you message all the time called Snoop Dodd.
Yeah. It's kind of creepy.
So you have a favourite person that you text and call a lot. Here's a record of that.
Yep.
Your text messages.
Yeah?
Mhm.
Just wondering if that's where you live.
That is not where I live. That is where is my most frequently texted person lives.
Ah.
We also had access to your camera phone.
What?
So we were able to take a photo from your phone.
Oh, wow, that's -- oh!
So this was from your camera.
Oh, wow.
We also had access to your microphone. We could have turned it on, listened to your conversations, even recorded them. We didn't.
Now I'm just going through my head, what else was I doing on my phone throughout the week, and I know it wasn't all good. So now it's like okay, they know.
What's going through your mind right now?
Uh... I have no idea how you guys have access to all my information. You guys could have taken pictures at the wrong time, could have listened to conversations that were private. Knowing where I'm gonna go or what I'm thinking because I'm sending it to a person via text is kind of unnerving for me.
You're pretty good at taking selfies.
Um, yeah, but I didn't --
Do you guys have-- so because I gave you access, you were able to access everything in my phone? Oh, wow, okay.
Keep in mind, these are very common standard terms and conditions.
Yes.
On apps that we all download all the time, you know, but we don't really think about just how much we're giving up in the process. We didn't dig deep into our testers' lives, we're just trying to show how invasive it can be.
It makes you feel violated, even though you accept a privacy policy, you're not thinking that they're going to have access to remote control into your phone. You're only thinking about hey, I want to use this app.
You also gave us permission to take a picture from your phone of you. And that's the picture that we took.
Okay.
We come from a time where just like we think we need these apps, though, I'm always holding this right now. If this wasn't in my hand, it feels weird, I feel naked almost, right?
As we reveal more details, it starts to really sink in.
We had the ability to own your phone. How are you feeling about that?
Like I need to do a better job than skimming.
Mhm.

Because I know that I did take a moment to like look for key words, and I just obviously didn't do quite a good enough job.

You basically broke my privacies just like the app did.

You accepted our terms, that's the thing.

Yeah, but we all accept terms and conditions, but it doesn't get displayed on TV. It is what it is, it already happened.

Why companies want so much access to our lives.

There is a lot of money in handling the personal information of Canadians, sometimes data is referred to as the new oil for companies.

Asha: Who's protecting your privacy?

We ask the man in charge.

Asha: This is marketplace.

We give up a lot of personal info when we download apps on our smartphones. From our text messages, call logs, photos, and more. So what are companies doing with all our data?

In general, we see that free apps are not really free. If we look at the real sense of the word. We expect them to be free because we're not paying for them, but that really means we're paying with our data.

Asha: App expert Domingo Guerra says companies could be collecting more data than they need so they can sell it.

So if the developer is going to sell your information to a third party like an advertising network, then having not just your name or your playing habits but also maybe your location is more valuable. So it helps the developer collect a higher price tag.

Asha: What are some of the privacy concerns when it comes to collecting this data?

There's a lot of unanswered questions as a consumer as to what is going to happen with our data, how long it's going to be kept, and if there's any way to delete it in the future.

Asha: Seems like companies have taken over our lives and our data. So what's being done to protect our information? We're paying a visit to Canada's privacy commissioner to find out.
Our app could access things like texts, phone calls, camera, microphone, GPS locator, the list really does go on. If you downloaded our app, we would have had access to all of that from your phone.

Mhm.

Doesn't that concern you?

Of course it does.

Asha: Daniel Therrien says that's why we all need to think before we install. And what about those lengthy agreements?

Companies should make better efforts to explain these. It means essentially shorter privacy policies or notices, perhaps concentrating on uses of information that the consumer would not expect.

Asha: It sounds like that falls on the companies, though. What are you as the privacy commissioner doing to lead the charge, to make sure that's happening?

One of the issues on which we're consulting is whether we should have stronger enforcement powers such as the authority to order companies to change their practices or even to issue fines, as many other countries in the US and western Europe can do.

Asha: On the US, the Federal Trade Commission has fined companies anywhere from $2,500 to $800,000 for privacy violations. And in Europe, they force businesses to reveal exactly where your information is going.

But Therrien says all he has the power to do is give out warnings. What can you say to Canadians who want you to do a better job in protecting their privacy?

I think we do a lot with the authority we have and even though all that we do under the current law is to make recommendations, this has resulted in changes in practises to companies.

Asha: Until there's more action on the federal front, sounds like it's up to us to police our own data.

You don't really know what you're agreeing to.

Asha: Back with our testers...

All right.

Here's my application manager. We're showing them how they can better protect their data right now.

All my apps are here. I click into Instagram.

Okay.
Permissions, and I'm able to turn off the camera if I want to, contacts, location, microphone, phone, SMS, storage.

Asha: Your app manager is the go-to spot to control what info you're giving out. And if there are apps on your phone that you don't use anymore, best to delete them because they could still be collecting your data.

Now armed with knowledge, there's only one thing left for our testers to do.

I'd like to ask you to delete the My Daily Horoscope app, please.

No problem.

Uninstall that.

Done and done.

Please remove that app from your phone, uninstall it.

With pleasure.

Send it to the garbage.

There's no such thing as a free app, you know that.

I know that.

We do have something for free today for you.

Okay.

And one for you, one for Snoop Dodd, if you want to check out what it says.

Yeah.

A marketplace t-shirt.

Okay.

And this one's for your favourite person.

Perfect.

I survived the marketplace mobile app.

I survived marketplace mobile app.

I survived the marketplace mobile app.

Good job.

I survived.

David Common: Next week, marketplace is on the move. Going undercover, tracking every step of a long-distance move.
That's our stuff sitting there in a movie theatre parking lot for an entire weekend. That's just unbelievable.

David: Misleading quotes, botched weights.

They were charging me four times the amount quoted, pretty much went into shock. Can you trust your mover?

You don't need a special licence. All that you simply need is a nice-looking website, a phone, and you're up and running.

Asha: Coming soon on marketplace. Online reviews, we all rely on them. But are they for real?

I was fooled by that. And I like to think of myself as an educated consumer.

Asha: We're searching for one of Canada's most popular online reviewers.

I've personally seen numerous people lose 9 to 11 pounds during their first week.

Asha: She sells hundreds of testimonials. Problem is, they're all fake.

I'm a certified financial advisor. And I'm a designer. And I'm a teacher.

Asha: We want to know why she does it.

Why do you do so many fake reviews, aren't you misleading people? I don't even know who you are.

Get away from my car.

Why won't you talk to us?