

Digital citizenship: Bringing digital activism home

By [Grace Cooper](#)

4 Oct 2019

In light of the Cambridge Analytica data breach, we should all take a more active role in our online activities.



Image credit: Carl Heyerdahl on Unsplash.

Got this social thing hacked, right?

Wrong, you and I, like many others may have been one of the 87 million people whose data was farmed and sold to Cambridge Analytica in 2017/2018. However, we can't be sure because, up until now, Cambridge Analytica has still not released the information they have procured.

The Netflix documentary, *The Great Hack*, was a mind-blowing exposé on the Cambridge Analytica saga, however, it doesn't really give us a way forward on how to be digital citizens while still protecting ourselves.



The Great Hack: A leadership, not data, crisis

Lisa Steingold 27 Aug 2019



I have a complicated relationship with the topics brought up. The digital field is my landscape and it is my job to draw on data for insights that give our clients the edge. Although it is not quite the same thing, what Cambridge Analytica was able to do with data is the holy grail of a digital campaign.

However, it still doesn't sit well. Is it ethics? A moral code that we all believe is meant to be adhered to? Or simply that it takes away a sense of agency that we all believe we have online?



Big Tech squeezes into small shoes as it denies being anti-trust

Derek Abdinor 23 Sep 2019



A public common with privacy issues

The digital world, and by extension social media, was built on a vision of the internet as a public common where knowledge could be shared, and connections easily made. The alleged scandals with Google and Facebook have highlighted the dark side of this ideology – one where we want free access but simultaneously desire privacy and autonomy.

The digital philosopher, father of virtual reality and author of *Ten Arguments for Deleting Your Social Media Accounts Right Now*, Jaron Lanier, has some profound digital ideas. However, deleting your social presence seems like an overreaction. An overreaction to an issue that is unlikely to go away simply because a few have chosen to opt out.

The main learning I have from him and other digital philosophers is that there is more that we, as ordinary citizens, can be doing. We need to start getting more actively involved, become digital activists. We need to start grappling with, not the issue of how social media affects the individual, but rather what the systematic effects are.

Digital agency

But, before we all become digital activists striving for privacy and protection on the world wide web, we need to start thinking about how we can take back the agency we seem to have lost, and how we can reduce the effect of bad actors on our lives. I will give two examples:

Last month, FaceApp, a mobile app, which uses artificial intelligence to generate realistic facial transformations trended on Twitter with users in South Africa sharing their aged pictures. Without reading the FaceApp terms and conditions.



FaceApp and the dark side of AI

Lee Naik 14 Aug 2019



What many don't realise is what you agree to when you use the app:

“ ...a perpetual, irrevocable, nonexclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, publicly perform and display your User Content and any name, username or likeness provided in connection with your User Content in all media formats and channels now known or later developed, without compensation to you. ”

What is a Russian-based company doing with your pictures, and shouldn't there be a law that makes it a requirement for them to tell you? More than anything, this kind of app shows the need for greater investment in digital citizenship because it is unlikely that many people understood what they were signing away.



Don't share everything on social media

4 Sep 2019



Another example, possibly more relevant to the average social media user, are those fun status updates on Facebook where you answer seemingly innocuous questions – your age, first job or mom's maiden name – and ask your friends to do the same in their own status.

Several of these fun, innocent questions are used as account verification questions also.

The screenshot shows the 'SECURITY QUESTIONS' section of a Facebook account. At the top, there is a link 'Change Questions...'. Below this, a list of six security questions is shown, with the first one selected and checked. The questions are: 'What is the first name of your best friend in high school?', 'What was the name of your first pet?', 'What was the first thing you learned to cook?', 'What was the first film you saw in the theater?', 'Where did you go the first time you flew on a plane?', and 'What is the last name of your favorite elementary school teacher?'. Below the list, there are two input fields labeled 'answer'. The first input field is empty, and the second input field is also empty. Below the input fields, there is a dropdown menu labeled 'Security Question 3' with a downward arrow. Below the dropdown menu, there is another input field labeled 'answer'. At the bottom of the form, there is a text box that says 'These security questions will help us verify your identity when you need to access your account or reset your password.' and two buttons: 'Cancel' and 'Continue'.

Just for fun, type 'copy and paste in your own status with your answers' into Facebook search and see how many of your contacts have posted this kind of thing publicly.

Selfies, Sexts and Smartphones, the phenomenal book by Emma Sadleir and Lizzie Harrison, quoted Frank Abagnale Jnr, security consultant and former con man in saying, if you share your date of birth and where you were born, he is 98% of the way to stealing your identity. Imagine how much more someone could do with all the answers to your accounts too.

So how to do we protect ourselves? The need for digital citizenship

The explosive growth of the digital realm has led to a lack of legislation and difficulty in setting enforceable laws. Digital citizenship, however, gives a framework for how to be an active participant while protecting yourself.

Simply deleting your online presence is not the solution.

The current digital existence is the way it is, however, as we assume a greater role and become global digital citizens, we can take our digital world from a place where companies like Google and Facebook can manipulate us to a place where we are more active, more constructive and more beneficial.

We want to create a better online experience, one in which we feel safe – which means we need to start having tough conversations about what digital citizenship looks like, and be honest about what our individual responsibilities are. But, that's the long-term goal.



Surviving the 'Digital App-ocalypse'

3 Oct 2019



In the short term, what are the easy wins in becoming a better digital citizen?

Number one, I urge you to sign the [petition](#), and help us find out what information Cambridge Analytica actually has.

Number two, Facebook recently introduced an '[Off-Facebook Activity](#)' feature that allows users to see the information that is collected by both themselves and third-party websites. Explore and understand what information social sites are farming on you.

And finally, number three, before you post anything, anywhere, just think about whether you would share that information in 'real' life. If you wouldn't, you probably shouldn't be posting it. This goes for anything from opinions on controversial topics to your security information.

For more information on digital citizenship, go [here](#).

ABOUT GRACE COOPER

Digital Content Curator at Joe Public Connect.
» Digital citizenship: Bringing digital activism home - 4 Oct 2019

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>