Google+ for journalists at risk

When they're creating new features, software designers talk in terms of "use cases." A use cas describes steps that future customers might perform with a website. "Starting a group with friends," would be a use case for Facebook. "Buying a book" would be case for Amazon's designers.

By Danny O'Brien 4 Jul 2011

When CPJ talks to Internet companies, we highlight the use cases of journalists who work in dangerous or authoritarian environments. It might be "defending against an attacker who has control of the infrastructure and wants my password." Or, it could be "breaking a controversial story to thousands of readers, which ma prompt government supporters to overwhelm the online complaint system." Or, "surviving a series of denia of-service attacks aimed at censoring my post."

Will be used in life-or-death situations

These are not the first scenarios a start-up might envision for their college-friend-sharing site or >text-message-your-friends service. Nonetheless, they're vital to consider. Whether it's Google in China, Twitter Iran, or Facebook in Egypt, if your social site becomes an essential part of people's lives, it will be used in life-or-death situations. Young but ambitious companies can anticipate and prepare for that.

And if reporters are an edge case, their experiences also shed light on the needs of other groups. For instance, journalists working on sensitive topics talk to a lot of people, often over email. It's vitally importan that those contacts aren't revealed to the wrong people, or that information isn't leaked about those conversations. Ex-partners of abusive spouses have a similar need, as they made very clear when Google Buzz abruptly broke that expectation of privacy. If Buzz had "reporters under threat" as a use case, perhap they might have spotted the other problem earlier.

Shaking out such unintended consequences is, I suspect, one of the reasons the company's new set of social projects, Google+, started with a smaller audience than Buzz. It's a complicated new product, and mapping all of those consequences will only slowly emerge through use. But having played with the servic for a few hours, I can offer some tentative analysis of how it may affect journalists - and by extension, the rest of us.

In emergencies, political or otherwise, one of the first acts of involved net users is to become a citizen journalist, if only for the duration. Everyone who speaks online potentially shares some of the use cases of threatened journalist. And the most at-risk journalists are canaries in the coal mine for grimly inevitable challenges that will face any successful Internet site.

How secure?

So, how secure is Google+ for at-risk reporters? From day one, everything on Google+ is encrypted with https. That means that no one, not even a maliciously motivated government with control of your local ISP, can intercept your private conversations. Companies like Facebook which did not start out using https struggle to implement it later. Some wealthy companies like Yahoo still haven't managed it, putting their webmail customers at constant risk of identity theft and surveillance.

What about leaked information about contacts, accidentally revealing who you talk and listen to? Like Twitter's "following" list, Google defaults to telling the entire world who is in your "circles" (its system for organising your friends and who you are following).

That makes sense for Google: The company is still attracting members for the service, and wants you to hunt through your friends' lists for new colleagues to add. But that's not a good default when a reporter, sa reaches out to a controversial activist, or reveals close family members.

Still, Google+ has learned the lesson of the Buzz fiasco, which is not to arbitrarily and automatically throw who Google thinks are your friends into this list. Even better, Google lets you select who appears in your public circle list. So a journalist can list all his or her public contacts, yet still reserve some for private connections. Boundaries like this will take some tending, and are prone to accidental revelation, but at leas you are not obliged to keep everything either private or public, a profound limitation for public writers involv in highly confidential conversations.

Use of pseudonyms

A topic that we've covered before is the use of pseudonyms on social networks. Facebook has a strict "re names" policy, which has had consequences in countries like pre-revolution Egypt, where large publicity-generating groups were removed because their owners wished to be anonymous, and for authors like Chinese writer Michael Anti, who prefer to use their well-known pen name over their real name. (Anti, by th way, has joined Google+.)

The rule for Google+ is subtly different: You should go by the name that you're usually known as, and that you should not impersonate others. We'll see how this plays out in practice. One possibility these rules co support is that users may have more than one Google+ account - a strategy Syrian activists have pursued Facebook, despite this being against the terms of service.

One boon for journalists isn't actually part of Google+, though it works closely with it. Google Takeout is th company's universal way for customers to extract for their own use all of the data the company keeps on them; it was rolled out for all Google services on the same day as the G+ test launch.

Google Takeout offers an opportunity to mitigate against the most drastic actions of Google itself. Like Facebook, Microsoft, Yahoo and other hosting services, Google will often decide to take down content it deems too controversial for their service. Putting aside whether these companies are right to remove photographs, groups, or news organisations, the more practical question is what journalists can do if their work is taken down. Or, for that matter, what journalists can do if they decide to move the material themselves.

Take your data, set up elsewhere

If your web hosting provider throws you off their computers, you want to at least take your data and set up your Internet stall elsewhere. In social networking environments like Facebook or Flickr, it's far less easy. A Michael Anti and Hossam el-Hamalawy discovered, if you leave, it can be very hard to get your content or contacts out of your former host.

Coded by the company's so-called "Data Liberation Front," Takeout is a tool that lets you download all you data into a format that you might carry to another service. (Facebook has an export tool, too, but it won't all you to obtain your contact's email addresses, thus reducing its usefulness outside of Facebook itself.)

It's too early to say whether Google Takeout will have more than a hypothetical benefit. Its usefulness depends on other services offering the capability to import the data that Google spits out.

Of course, it's too early to tell anything about Google+. Will it be successful enough to be considered a journalist's tool? Will it stumble like Google Wave and Buzz? Will it change the world, or remain a geeky backwater?

Strong incentives

It looks like Google has considered some of CPJ's use cases when building Google+, and has strong incentives to fix any other issues before they become a bigger problem. (The company is a member of the Global Network Initiative and also paid US$8.5 million in a class action settlement over Buzz's privacy violations.)

With this launch, Google is clearly thinking big. And when a company thinks big for its products, it should a think about the ethical and privacy ramifications of thinking big. People's livelihoods, the openness of their societies, and even their lives may depend on it.

Article published courtesy of CPJ

ABOUT THE AUTHOR

San Francisco-based CPJ internet advocacy coordinator, Danny O'Brien has worked globally as a journalist and activist covering technology and digital rights. Follow him on Twitter [[@danny_at_cpj]].