CLOUDY CLOUDS

This is in response to *Computer*'s April 2014 Computing and the Law column ("Readers Choice"), in which Brian Gaff discusses recent changes in patent law. I am an IEEE member and attended the Software Technology Conference (STC) in Long Beach, California, on 31 March–3 April 2014.

The conference organizers covered lots of topics, including big data and cloud computing. When I worked as an engineer at Boeing, I helped architect and build datacenters for Boeing and government programs that are now called clouds. These clouds contained Boeing proprietary data.

I asked this question at the IEEE STC conference but did not, in my opinion, receive a good answer: "If proprietary or patent-type data is stored in a noninternal cloud, does it also belong to the cloud owner?"

With big data and clouds playing a greater role in the data and storage world, I think the users who pay for capability and data storage in a cloud should have some understanding of the control over their data. For example, if the cloud were hacked and the user's data stolen, what would be the outcome?

Perry Towles
perry@towles.com

The author's response:

To summarize, your question is, "If proprietary or patent-type data is stored in a noninternal cloud, does this also belong to the cloud owner?"

Don't assume that data you store in the cloud remains your exclusive property. The answer to this question will depend on the service agreement that you have with the cloud provider. If the agreement gives the provider ownership rights in the data, then there could be issues with continuing to access your data if, for example, you decide to change providers. Also, if you store proprietary or confidential data in the cloud, you might need to ensure that no one else—including the provider—has access to that data.

Make sure that you understand the terms of the service agreement before committing to use cloud-based services. Have your lawyer read the agreement and include language that protects your data and your interests.

Brian Gaff
bgaff@mwe.com

SNOWDEN'S LEGACY

I'm somewhat astonished at Hal Berghel's column, "Mr. Snowden's Legacy," in the April 2014 issue. Not that it wasn't cogent and important: it was both.

I am just surprised to see such an article in a technology periodical the likes of *Computer*. I have always assumed that the flagship magazines of IEEE and ACM would intentionally steer well clear of anything that can be construed as overtly "political." It's a constraint that may be misplaced in certain situations; though I can see the rationale from the perspective of the magazines' editors—even a small step over the line into the current polarized whirlpool of American politics, and who knows what the unintended consequences might be?

I don't think that software and technology can be kept separate and carefully compartmentalized from other aspects of our daily lives. Professor Berghel's elegant dissection of the reasons for the visceral reaction to Mr. Snowden's disclosures was logical, well-reasoned, and informative. It should make some people think—well, perhaps those people who have not already completely made up their minds on the subject.

I wonder if the publication of "Mr. Snowden's Legacy" might herald more political science–related offerings among the normal computer science fare in these professional journals? And I wonder what the reaction might be from Certain Quarters?

There are many aspects of modern life and social trends that are outside the strict confines of technology, about which computer folk might have valuable input. Those in other disciplines, such as the Union of Concerned Scientists, have stepped up to this challenge; perhaps Berghel's article will lead software practitioners to let their voices be heard on other topics.

Phillip G. Armour
armour@corvusintl.com

The author's response:

Thank you for the supportive letter. In it you raise several interest-

 Published by the IEEE Computer Society

ing issues. There is no question that publishers have always been incentivized to avoid controversial topics not of their choosing. In the early days of "yellow journalism," the larger media outlets were either owned or controlled by wealthy patrons who used their media as a bully pulpit to advance their personal agendas.

These days, mainstream media is beholden to advertisers, corporate owners, and the interests of their board members, while professional publications are beholden to individual and institutional members and subscribers. But overall, the default state for publishers has been and continues to be risk aversion. That has always had a stultifying effect on investigative journalism, but the revenue decline starting in the 1970s pretty much delivered the death blow.

Newsrooms continue to close, and media independence is all but gone through corporate takeovers and mergers. The combined effect of these forces has been to narrow the scope of genuine reporting and has led to the displacement of the Fourth Estate by the Fifth. Mainstream media these days is entertainment—and I use that term charitably.

I can confirm that the political whirlpools of which you speak—and the consequences resulting therefrom—are very real. Dealing with controversy isn't for the faint of heart. There are many people who don't like to see questions asked that threaten their preconceived answers. But solipsism isn't a viable response when faced with ubiquitous digital dragnet surveillance by both government and private contractors, the harvesting of personally identifiable information by virtually every company that has a computer and access to the Internet, universal monitoring of communications, and, lately, aerial surveillance by drones.

And it's through the efforts of technologists like us that this is possible. We all owe it to future generations to critically assess the potential consequences of our actions. I believe the role of a columnist is to continuously encourage self-assessment and to remind our constituencies that not everything we can do is worth doing.

Given the exceptionally high educational attainment of our peer group it's possible to find technical solutions that are compatible with a constitutional framework. But that won't happen automatically. People have to be challenged to look for them. This is exactly what the high-tech executives didn't do when they so willingly, and without legal requirement, gave away customer information to the NSA for the PRISM program. There is little evidence of any penetrating introspection—with the possible exception of Steve Jobs.

I frequently link to definitive reports provided by the Federation of American Scientists, especially their strategic security program (www.fas.org/programs/ssp/index.html). Their attempt to preserve official documents for history is to be commended. In my opinion, all technical and professional societies have an obligation to engage in some way with the important contextual issues to which their members contribute.

Columnists play an important role in holding a mirror up to their profession. I am very fortunate for the leadership of the editor in chief and editorial board of *Computer*, who allow me to do just that.

Hal Berghel
hlb@computer.org