April 2018

#FixFacebook

Sites like Facebook urgently need to get their act together. The Cambridge Analytica debacle is only the tip of the iceberg and the Social Media giants, as well as the leading search engine providers, have built their houses on shaky foundations.

As Facebook and Twitter scramble clumsily to address the huge reputational harm they have suffered during the recent election 'hacking' and Cambridge Analytica data exploitation fiascos, these leading social media sites appear to be missing some very basic points.

There is no question that sites like these have been hugely successful, yet there are glaring and very basic security holes in their models that informed observers have long debated. What these are, and how they might be fixed, are points rarely acknowledged by the firms and the supposed solutions now being announced to address the current storm of controversy about their ethos, operations and controls fail to adequately address them.

1. Identity verification

Estimates vary, but sites like Facebook, LinkedIn and Twitter are often riddled with fake, duplicate or partially falsified profiles. I have seen figures stating that between 5% and 10% of accounts are fakes on some major sites. The true numbers are probably higher. Many of these fakes are used by fraudsters and other criminals, either to find or to con victims. Others are used by Bots, stalkers, and more are frequently setup by angry ex-partners seeking revenge. I recently worked on a case in which a 19-year-old hairdresser had managed to create 42 sophisticated fake profiles on one leading site which she then used to target her ex-boyfriend’s new partner.

Sites like Facebook have a clear duty of care to their users, given that they have encouraged them to post a raft of personal details online, thus exposing themselves to exactly this type of risk.

One obvious way to improve security would be to add *optional* identity verification that conforms to online banking standards; give me the *choice* to validate myself. If I choose to do so, allow me to then block and un-friend, with one click, anyone who has not also opted to validate themselves, then automatically prevent any unvalidated user from messaging me, friending me or viewing my profile in the future.

Let’s have two communities on Social Media; those who are willing to validate themselves and who share a desire for better security, and those who do not wish to do so, who share a desire for anonymity. The two should probably not be mixing. #SocialFork.

2. Opt-out vs. Opt-in to security

Currently, Facebook’s users, for example, must work through a long list of security options and then opt-in to many of the more secure settings. This is the reverse of every security protocol I have ever seen and flies in the face of common sense.

Every user should be assigned the most secure settings by default and if the sites don’t want to adopt this standard, then regulators must force them to do so. Let users opt-out of security if they so wish but ensure that they explicitly accept the resulting risks when they make this choice. #ProtectMe.

3. Users are not merely ‘identity capital’

The social media market has long regarded its users as capital, as a commercial asset, and not as customers. This is why the sites are generally free to use; the paying customers are the corporate firms and governments that want the benefits of the Big Data sets created by these sites. This needs to change. If my data is of value to Facebook, Twitter or LinkedIn etc, then we can only draw one of two conclusions:

1. I am a customer and I am *paying* for my access to the service *with* my data, or;
2. I am a *stakeholder* and I am due a *share* of the value derived from the monetization of my data.

Any other model is unjustifiable and constitutes exploitation of gullible citizens by a large corporation. This is the kind of corporate misconduct that government regulators are paid to identify and then address. Let's see more of that please. #Payback

Sites like Facebook must now get their act together. Let me assure you that the Cambridge Analytica debacle is only the tip of the iceberg and Social Media giants, as well as the leading search engine providers, have built their houses on shaky foundations. It's time they mended their ways or paid the long-overdue price.

The Wild West days of unbridled data exploitation and an out-of-control Big Data market are likely to end, and fundamental change is on the way, as regulators around the world finally wake up from a decade-long slumber and embrace their own duty of care. We can already see users gaining much greater control over who can see what; witness Google's account clean-up initiative. Expect to see a large segment of the user base sharing less and only sharing with a tighter circle of friends. And expect to hear an increasing clamour from lobbying groups presenting users' claims for a financial stake in the huge mountain of personal and lifestyle data we choose to post online and which we could very easily decide to stop posting. #Post-It-Not.

Mark Johnson is a security veteran with 40 years international experience in the military, drug enforcement, high tech crime control and internet investigations arenas.

www.linkedin.com/in/markjohnsontrmg/