net.wars - www.pelicancrossing.net/netwars/2017/09/equifaction.html

Equifaction

The Equifax announcement this week is peculiarly terrible. It's not just that 143 million Americans and uncertain numbers of Canadians and Britons are made vulnerable to decades of identity fraud (social security numbers can't - yet - be replaced with new ones). Nor is it the unusually poor apology issued by the company or its ham-fisted technical follow-up (see also Argentina). No, the capper is that no one who is in Equifax's database has had any option about being in it in the first place. "We are its victims, not its customers," a number of people observed on Twitter this week.

Long before Google, Amazon, Facebook, and Apple became GAFA, Equifax and its fellow credit bureaus viewed consumers as the product. Citizens have no choice about this; our reward is access to financial services, which we *pay* for. Americans' credit reports are routinely checked on every applications forcredit, bank accounts, or even employment. The impact was already visibly profound enough in 1970, when Congress passed the Fair Credit Reporting Act. In granting Americans the right to inspect their credit reports and request corrections, it is the only US legislation offering rights similar to those granted to Europeans by the data protection laws. The only people who can avoid the tentacled reach of Equifax are those who buy their homes and cars with cash, operate no bank accounts or credit cards, pay cash for medical care and carry no insurance, and have not need for formal employment or government benefits.

Based on this breach and prior examples, investigative security journalist Brian Krebs calls the credit bureaus "terrible stewards of very sensitive data".

It was with this in the background that I attended a symposium on reforming Britain's Computer Misuse Act run by the Criminal Law Reform Now Network. In most hacking cases you don't want to blame the victim, but one might make an exception for Equifax. Since the discussion allowed for such flights of fancy, I queried whether a reformed Act should include something like "contributory negligence" to capture such situations. "That's data protection laws," someone said. True. Later, however, merging that thought with other comments about the fact that the public interest in secure devices is not being met either by legislators or by the market inspired Duncan Campbell to suggest that perhaps what we need as a society is a "computer security Act" that embraces the whole of society - individuals and companies - that needs protection.[1] Companies like Equifax, with whom we have no direct connection but whose data management deeply affects our lives, he suggested, should arguably be subject to a duty of care. Another approach several of those at the meeting favored was introducing a public interest defense for computer misuse, much as the Defamation Act has for libel. Such a defense could reasonably include things like security research, journalism, and whistleblowing,

The law we have is of course nothing like this.

As of 2013, according to the answer to a Parliamentary question, there had been 339 prosecutions and 262 convictions under the CMA. A disproportionate number of those who are arrested under the act are young - average age, 17. There is ongoing work on identifying ways to turn the paths for young computer whizzes toward security and societal benefit rather than cracking and computer crime. In the case of "Wannacry hero" Marcus Hutchins, arrested by the FBI after Defcon, investigative security journalist Brian Krebs did some digging and found that it appears likely he was connected to writing malware at one time but had tried to move toward more socially useful work. Putting smart young people with no prior criminal record in prison with criminals and ruining their employment prospects isn't a good deal for either them or us.

Yet it's not really surprising that this is who the CMA is capturing, since in 1990 that was the threat: young, obsessive, (predominantly) guys exploring the Net and cracking into things. Hardly any of them sought to profit financially from their exploits beyond getting free airtime so they could stay online longer - not even Kevin Mitnick, the New York Times's pick for "archetypal dark side hacker", now a security consultant and book author. In the US, the police Operation Sundown against this type of hacker spurred the formation of the Electronic Frontier Foundation. "I've begun to wonder if we wouldn't also regard spelunkers as desperate criminals if AT&T owned all the caves," John Perry Barlow wrote at the time.

In the UK, the prosecution of Schifreen and Gold, who were busted for hacking into Prince Philip's Prestel mailbox, established the need for a new law. The resulting CMA, despite amendments in the years since (DDoS attacks were added in 2006), was not written for a world in which everyone is connected, street lights

[1] Although discussion at the symposium was subject to Chatham House Rules, Duncan Campbell consented for me to reference him on this point.

have their own network nodes, and Crime as a Service relies on a global marketplace of highly specialized subcontractors. Lawmakers try to encode principles, not specifics, but anticipating such profound change is hard. Plus, as a practical matter, it is feasible to capture a teenaged kid traceable to (predominantly) his parents' basement, but not the kingpin of a worldwide network who could be anywhere. And so CLRNN's question: what should a new law look like? To be continued...

Author: Wendy M. Grossman

Wendy M. Grossman is the 2013 winner of the Enigma Award*. Her* Web site *has an extensive archive of her books, articles, and music, and an* archive of earlier columns in this series*. Stories about the border wars between cyberspace and real life are posted occasionally during the week at the* net.wars Pinboard *- or follow on* Twitter*.*