At Issue

Lee Goldberg, Editor

Has Technology Become the Enemy of Democracy?

Since March is Women's History Month, I was all set to write an inspiring editorial about the growing presence of women in tech-related fields and some of their accomplishments. Then the word came out that a small company in England had managed to weaponize the personal data it had hijacked from 50 million Facebook users in an attempt to influence America's presidential election. Even if Cambridge Analytica's psychological profiling techniques were completely ineffective, it was a chilling assault on our democratic system. Worse yet, it's only one of many examples of how technology seems to be making it harder for free, open, and democratic societies to function.

Allowing companies like Facebook, Google, and Amazon to collect and use personal data with few meaningful restrictions has made e-commerce incredibly efficient and enabled the creation of many innovative services. Unfortunately, the same liberties that allowed them to build up detailed e-dossiers had few, if any, restrictions against their abuse. Keep in mind that the 2016 elections were a relatively early-stage Beta test of a new form of information warfare that will only get more effective and difficult to combat the longer it has free run of our society and our economy.

It appears to me that there are few, if any, legal or technical measures in place to prevent these, or other types of corporate malfeasance. The mountains of information about purchases, locations, travel, social media posts and social connections could easily be turned into economic, behavioral, psychological and perhaps even political profiles that identify desirable – or undesirable - tendencies that would be of interest to a business or industry. It's not inconceivable, for example, for a company to apply AI and Deep Learning, and other analytic techniques to extract patterns from the data that businesses like insurance companies and mortgage brokers, or potential employers could use to avoid having to deal with "undesirable individuals".

I also worry that the same information, and many of the same analytic tools, could be easily fashioned into a behavioral surveillance system that would be the envy of any would-be dictator. Even without access to the massive databases currently being maintained by official government agencies, it would become fairly easy to create an extra-governmental system that keeps tabs of "suspicious" behavior, however the user chose to define it.

Before you dismiss this as paranoid ramblings, consider the fact that such a system is already in place in parts of China. A cooperative venture between the Chinese government and several of the country's largest banks, the so-called "Social Credit System" generates a three-digit social credit score for each citizen that determines their eligibility for everything from jobs and housing to which schools their children are allowed to attend. The score is calculated based on a large matrix of personal data that includes your purchases (including titles of books and videos), where you went to school, the type of car you drive, your online activity, and who (and where) you spend time with.

While only deployed in parts of China today, the government has announced that they intend to roll it out for all Chinese citizens by 2020. And if there is any question about the intent of the system, Wired Magazine reports that "China's State Council has signaled that under the national social credit system people will be penalized for the crime of spreading online rumors, among other offenses, and that those deemed "seriously untrustworthy" can expect to receive substandard services[1]."

I don't think that most Americans would knowingly allow such a system to be created here, but with so many of the elements required to build it already in place, all it would take would be the right financial incentives and a small spark of fear, perhaps generated by an act of terrorism, to get things rolling. We saw how the attacks of September 11, 2001 gave rise to a massive expansion of America's electronic surveillance infrastructure and a greatly relaxed interpretation of the FISA Act of 1978 that protected us against privacy abuses by our government[2]. Is it too far-fetched to consider the possibility that that some well-intentioned security agency might find a way to use commercially collected data to supplement their own records collected from Internet communications and facial recognition systems?

The good news is that these alarming scenarios are probably not inevitable.

We still have time to develop technical measures and laws that will preserve our rights, freedoms, and ability to function as informed participants in a functioning democracy. Nobody has all the answers yet, but we can take a lead from some countries in Europe that already have laws in place to protect people's personal data. I also suspect some important parts of the solution will emerge from the same entrepreneurial culture that brought the Internet, social media and e-commerce to the world.

As technologists, I believe that we can be part of the solution.

Is our democracy in danger from abuse of social networks? If so, what can we do about it? Please share your thoughts with me, and your fellow readers, by writing me at: lee.goldberg@advantagemedia.com

[1] Inside China's Vast New Experiment in Social Ranking – Mara Hvistendahl – Wired, December 2017.

[2] Foreign Intelligence Surveillance Act of 1978 ("FISA") created as a response to President Richard Nixon's usage of federal resources, including law enforcement agencies, to spy on political and activist groups within the U.S. https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act

PRODUCT DESIGN & DEVELOPMENT
73rd Year, Issue 1

Editorial Director | JOYCEANN GARIPPA
joyceann.garippa@advantagemedia.com

Editor-in-Chief | LEE GOLDBERG
lee.goldberg@advantagemedia.com

Managing Editor | SPENCER CHIN
spencer.chin@advantagemedia.com

Sr. Reporter | MEGAN CROUSE
megan.crouse@advantagemedia.com

Design Engineering Group
SALES & EDITORIAL OFFICE
100 Enterprise Drive, Suite 600,
Rockaway, NJ 07866
Phone: 973.920.7000

NICK PINTO
Vice President of Business Development,
nick.pinto@advantagemedia.com
973-920-7746

GLEN SUNDIN
Vice President of Strategic Accounts
glen.sundin@advantagemedia.com
973-920-7038

JOE DEL GROSSO
Regional Director of Sales
joseph.delgrosso@advantagemedia.com
973-920-7192

TIM OWCZARZAK
Regional Director of Sales
Tim.O@advantagemedia.com
973-920-7747

PAT VENEZIA
Regional Director of Sales
Pat.Venezia@advantagemedia.com
973-920-7467

MAUREEN ELMALEH
Regional Director of Sales
Maureen.Elmaleh@advantagemedia.com
973-920-7686

Advantage Business Media

Chief Executive Officer
JIM LONERGAN

Chief Operating Officer/Chief Financial Officer
THERESA FREEBURG

REPRINTS
The YGS Group
800.290.5460
reprints@theygsgroup.com

SUBSCRIPTIONS/CHANGE OF ADDRESS
Please visit: www.pddnet.com/contact-us

LIST RENTALS
Infogroup Targeting Services
Senior Account Manager, **Bart Piccirillo**
402.836.6283; bart.piccirillo@infogroup.com
Senior Account Manager, **Michael Costantino**
402.863.6266; michael.costantino@infogroup.com