2015

Digital Laws Evolve

Neil M. Richards
Washington University in St. Louis School of Law, nrichards@wustl.edu

with fake online profiles that have convincing backgrounds and histories. The software will allow US service personnel to operate up to ten separate false identities based all over the world from their workstations "without fear of being discovered by sophisticated adversaries". These personas allow the military to recruit, spy on and manipulate peoples' behaviour and ideas.

Such projects represent the first wave of computational propaganda, but they are constrained in their scale (and ultimately their effectiveness) by the simple fact that each profile has to be driven by an actual human on the other side. In 2015, we will see the emergence of more automated computational propaganda – bots using sophisticated artificial intelligence frameworks, removing the need to have humans operate the profiles. Algorithms will not only read the news, but write it.

These stories will be nearly indistinguishable from those written by humans. They will be algorithmically tailored to each individual and employed to change their political beliefs or to manipulate their actions. Already, Mexican drug cartels have employed propaganda bots to target messages at individual members of the public, to convince them that the death of a journalist in Las Choapas had nothing to do with hit men employed by the gangs. This type of propaganda can be produced at an almost limitless scale using the estimated ten million social-media bots. Such bots are currently available for rent on online hacker forums for between $5 and $200 per thousand, depending on how "human" – and therefore how effective – they appear.

The Russian foreign intelligence service has announced a 30-million-ruble (£500,000) contract for the "development of special software for automated information dissemination in major social networks". In 2015 we will also see the first results from initial field tests of the US IARPA (Intelligence Advanced Research Projects Activity) project to deploy propaganda bots in South America in an attempt to influence local political opinion.

SPOT ILLUSTRATION: JAMIE JONES

MIXED RESULTS

Eight "Millennium Development Goals" were outlined by the UN in 2000, with a deadline of 2015. Some nations did well – China reduced its population in poverty by half – but globally, results are less promising: 162 million children will still go hungry. Thomas Hale

It is still early days – many of the bots deployed in 2015 will be programmed to use relatively simple heuristic techniques to imitate intelligence. But, powered by rapid advances in artificial intelligence, propaganda bots will soon run on genetic algorithms that let their ideas and messaging evolve, based on the resonance and effectiveness of previous messages. We are likely to see versions of these bots deployed on US audiences as part of the 2016 presidential election campaigns, and not only by the traditionally more tech-savvy Democrats.

This technology exploits the simple fact that we are much more impressionable than we think. Facebook's recent experiments to modify users' moods show us that the very language we use to communicate is subject to manipulation based on the stories that the Facebook algorithm chooses to show us. Furthermore, researchers at MIT have shown that a false upvote cast early on can improve the public response to a story by 25 per cent; a single early downvote can make an otherwise good story be perceived as a low-quality piece of journalism. In 2015, the propaganda bots will start to use this knowledge to influence news feeds – automated "friends" will like, retweet and comment on stories that are in line with their propaganda goals.

We can also employ bots to help us determine if there are attempts at propaganda underway. Reactions to the downing of Malaysian Airlines flight MH17 over Ukraine show that the Russian and US media want the global audience to view things differently. We can employ algorithms to monitor mainstream media messaging out of Russia, compare that to what we are seeing in the US outlets, and flag substantive differences in language. We can also employ bots to monitor all of the millions of edits that happen daily on sites such as Wikipedia and uncover attempts to change language from "terrorists" to "Ukrainian soldiers", though it won't tell us which version is true. For that we still need humans to weigh the evidence.

Sean Gourley is CTO of Quid, an augmented intelligence company

1.4 MILLION

–

Predicted Ebola infections in West Africa by 2015, according to the US Centers for Disease Control and Prevention. A US-developed vaccine is due that year.

DIGITAL LAWS EVOLVE

As big data seeps into every aspect of daily life, the law will catch up and introduce a raft of essential new e-regulations

By **Neil M Richards**

THE LAW HAS ALWAYS BEEN SLOW to keep up with technology, but in 2015 we will see increasing regulation. Over the past decade, as the web, social, mobile, cloud and big data phases of the digital revolution have leapt forward, regulators have been reluctant to intervene. After all, law can be a blunt tool, and

it is all too easy for even well-meaning lawmakers to issue rules that later turn out to be restrictive.

But as the scope and scale of the digital transformation has become apparent, regulators have woken up. Surveillance reform is on the agenda around the world, and so is privacy law more generally, such as the revision of the EU Data Protection Directive and serious efforts at reform by the White House, the Federal Trade Commission, and other parts of the US government. The decision by a Spanish court earlier this year requiring Google to filter its search results to protect privacy under what is colloquially known as "the right to be forgotten" is part of this trend.

But more change is on the horizon. Surveillance law will adapt to include the cloud, and it will no longer be acceptable for governments to use "we collected the data because it wasn't prohibited" or "anything shared on the internet is fair game" as a viable excuse for intrusions into their citizens' privacy.

As big-data predictions start to affect more of our lives, we'll see new protections come into force against discrimination by algorithm, whether by security services, insurance companies or employers. As the sensor-enabled "internet of things" promises to turn every electrical device (and quite a few that aren't) into a data-collecting networked appliance, and as smart watches and wearable tech such as Google Glass proliferate, we'll need rules for the data that is collected: who owns it, for what purposes and for how long? As long as technology was largely confined to cyberspace, it was relatively easy to keep things separate. But as our digital technologies increasingly enter physical space, law will find itself entangled in these new and important questions – whether it wants to be or not. Already, companies are starting to hire "chief privacy officers" in record numbers, and new law graduates throughout the western world are finding that the high-growth area within law firms is in its privacy-law practices.

LAND GRAB

–

In 2015, China will complete a round of island-building in the South China Sea, turning reefs into atolls to bolster its claims to valuable strategic maritime territories. TH

We have seen this pattern before. At the very dawn of the digital age, cyber-utopians argued that law had no place in our new digital realm. But, as it turned out, laws were in fact necessary – to provide a basis for digital property and digital commerce; to provide security from scammers and malicious hackers; and for the redress of the many crimes and wrongs that would inevitably occur as major chunks of human life migrated to digital formats. The best example of this was in the area of copyright, when perfect, cost-free digital copying threatened the long-established economic model of many of the industries that make culture: music, books and film. For a while, we stared into the abyss of a revolutionary Napster and YouTube future, and then we pragmatically backed away, bringing copyright law into the digital realm. Many of us believe that copyright law actually went too far, but the clear lesson is that if law can regulate copyright for the entertainment industries, it can – and should – regulate data for everyone else.

And it will. As the digital revolution proceeds, we're realising that we have a right to demand that privacy, security, expression, equality and other values we fought so hard to get built into the democratic society of the twentieth century get built into the digital one of the twenty-first. In 2015, these developments will kick into high gear, and law will start to catch up with technology.

Neil M Richards is professor of law at Washington University