Views

Vincent Blondel

Leila Takayama

Bruce Schneier

COMMUNICATIONS

Data Sources

Mobile phones are great sources of data—but we must be careful about privacy, says Vincent Blondel.

Anyone who has worked with mobile-phone data knows how incredibly useful such information can be, even when it's anonymous. It is amazing—but at the same time frightening—what massive amounts of spatiotemporal data points from mobile phones can tell about ourselves, our lives, and our society in general.

Mobile phones know where we are and when, and whom we talk to. In some cases they even know when and in what amounts we add credit to prepaid phones, which in some places is a good proxy for how much money people have. All this data can be harnessed for the public good (see "Big Data from Cheap Phones," page 50). In countries where even population estimates are hard to get, mobile phones constitute a unique source of information.

Recently, the telecom operator Orange challenged researchers around the world to analyze "anonymized" mobile-phone data sets from Ivory Coast and see how the information might be used. The data sets are based on more than two billion records of communications between five million customers in the African country.

This "data for development" challenge—the first of its kind—has been received with tremendous enthusiasm. Over the last six months, hundreds of researchers have proposed ideas that are creative, original, and useful. Among many others, they suggest ways to respond to emergencies, improve health, optimize transportation infrastructures, monitor development policies, prevent violence, and anticipate the spread of diseases such as meningitis, malaria, or cholera.

Unfortunately, such data can potentially be misused, and making the information available could compromise the privacy of mobile-phone customers. A few data points suffice to identify most customers, even if their names are stripped from records. But at the same time, those data points may save their lives, or at least help make those lives better and safer. These trade-offs should be worked out and debated so that we can benefit from data in a way that respects the interests of all.

Vincent Blondel is a professor of applied mathematics at Université Catholique de Louvain in Belgium and research affiliate with the Laboratory for Information and Decision Systems at MIT.

ROBOTICS

Friendly Machines

Making human-friendly robots is a pressing challenge and a big opportunity, says Leila Takayama.

As a research scientist studying human-robot interaction, the most frequent question I hear is: when are your robots going to replace me? But that is certainly not my goal.

A more important objective, to my mind, is making robots more human-friendly, in terms of form, behavior, and function, so that they can work more effectively alongside people (see "Baxter: The Blue Collar Robot," page 38). By this I mean that robots should be appealing and approachable. They should behave in ways that are easy for humans to interpret, and they should perform functions that meet real human needs.

This is not about making human-like robots. Humanoid robots have a place in

SAM KERR

entertainment, medical training, and possibly other domains, but human-friendly robots are not necessarily humanoid. In fact, by setting user expectations too high, looking too human could make it more difficult for a robot to interact with people. We are often disappointed and frustrated with the limited capabilities of robots that look as if they should be just as smart as we are.

These robots also do not need to behave just like humans. They might, for example, behave more like service dogs. As long as they are predictable, robots have a hope of making it in the everyday world. Many people know how to communicate with dogs just fine without needing language at all.

Finally, these human-friendly robots must meet real human needs, not only the needs of their inventors. Fetch-a-beer and fold-a-towel demos are nice scientific steps toward building more general robotic capabilities. But what we need now is for human-centered-design researchers and product-minded entrepreneurs to do the dance of the necessary and the possible with the robotics community.

Why does this humanist stuff matter? Because it will help us realize the true potential of the technology. Too many long-term studies of robots in hospitals, offices, and homes have revealed the problem with ignoring the importance of human-to-robot interaction: the robots end up interred in closets, retired to garages, or "mysteriously" disabled and shoved under desks.

Many of my robotics colleagues cringe at the challenges presented by unstructured environments that personal robots need to navigate. But the untrained people around these robots present an entirely different set of equally important challenges. Without serious involvement from the interaction design, product design, and entrepreneurial communities, personal robots don't stand a chance of surviving out in the "real world."

Leila Takayama, a member of MIT Technology Review*'s Innovators Under 35 list in 2012, is a research scientist and manager at Willow Garage.*

INTERNET

Online Nationalism

The rhetoric about "cyberwar" is getting out of control, says Bruce Schneier.

For something that was supposed to ignore borders and bring the world closer, the Internet is fostering an awful lot of nationalism right now. We're seeing increased concern about where IT products and services come from: U.S. companies are worried about hardware from China, European companies are worried about cloud services in the U.S., and Russia and China might each be building their own operating systems to avoid using foreign ones.

I see this as an effect of the saber-rattling that has been going on. The major nations of the world are in a cyberwar arms race, and we're all being hurt by the collateral damage.

Our nationalist worries have recently been fueled by reports of attacks from China. These attacks aren't new—cybersecurity experts have been writing about them for at least a decade, and the most recent allegations aren't very different. This isn't to say that the Chinese attacks aren't serious; the country's espionage campaign is sophisticated. But it's not just China. All governments have discovered the Internet; everyone is spying on everyone else. China is certainly worried about the U.S. Cyber Command's recent announcement that it was expanding from 900 people to almost 5,000, and about the National Security Agency's massive new data center in Utah.

At the same time, many nations are demanding more control over the Internet within their borders. They reserve the right to spy and censor, and to limit the ability of others to do the same.

But remember: this is not cyberwar. It's espionage, something that's been going on between countries ever since countries were invented. Yet the rhetoric we're hearing is of war.

Unfortunately, that plays into the hands of the military and corporate interests that gain power and profit from the cyberwar arms race in the first place. The more we believe we are "at war," the more willing we are to give up our privacy, freedoms, and control over how the Internet is run.

Arms races are fueled by two things: ignorance and fear. We don't know the capabilities of the other side, and we fear that they are more capable than we are. So we spend more, just in case. The other side, of course, does the same. That spending will result in more cyberweapons for attack and more cybersurveillance for defense. It will result in move government control over the protocols of the Internet, and less free-market innovation in the same arena.

At worst, we might be about to enter an information-age Cold War: one with more than two "superpowers." This is inherently destabilizing. It's just too easy for this amount of antagonistic power and advanced weaponry to get used: for a mistaken attribution to be reacted to with a counterattack, for a misunderstanding to become a cause for offensive action, or for a minor skirmish to escalate into a full-fledged cyberwar.

Nationalism is rife on the Internet, and it's getting worse. We need to damp down the rhetoric.

Bruce Schneier is chief security technology officer of BT.