

e-outed

EVGENY MOROZOV

Helen Nissenbaum

PRIVACY IN CONTEXT

Technology, policy, and the integrity of social life
304pp. Stanford University Press. \$70; paperback,
\$24.95; distributed in the UK by Eurospan. £57.95;
£20.95.

978 0 804 75237 4

Is privacy outdated? Mark Zuckerberg, the twenty-five-year-old founder of Facebook, sees nothing wrong with his company's aggressive attempts to make user data more public, arguing that social norms have evolved and less privacy is what users want. A growing number of companies build their business models on the premiss that privacy is dead. Blippy.com (launched in December) allows users to share details of their credit card transactions online (more than 5,000 users have already done that). Jigsaw.com pays users one US dollar per entry when they upload contact details of people they meet (the site has 20 million contacts and adds 25,000 new contacts every day). Only the intervention of the Information Commissioner's Office delayed the launch of Internet Eyes, a new website that promised members of the public cash prizes for monitoring commercial CCTV footage from across the UK (more than 13,000 people registered with the site nevertheless).

But have our values really changed? And should it be a cause for concern, if they have? According to Helen Nissenbaum in her excellent new book *Privacy in Context: Technology, policy, and the integrity of social life*, the information revolution has been so disruptive and happened so fast – Facebook and YouTube are just six years old – that the minuscule and mostly imperceptible changes that digital technology has brought to our lives may not have properly registered on the social radar. Radio Frequency Identification technology (to be found in electronic passes, such as Oyster Cards) and computerized databases had been scrutinized by privacy advocates even before Mark Zuckerberg was born, but the invention of the internet, accompanied by vast improvements in hardware and software, have triggered a new, unprecedented wave of concerns. Storage capacity and access to information have become very cheap, producing a number of data aggregation companies that sell access to databases which contain exhaustive information of the most banal variety (AutoTrackXP, one such search service, offers “billions of current and historical records on individuals and businesses”). The rise of search engines, blogs and social networking sites have also made information more mobile, setting it free from the dull databases, and empowering armies of geeks to “remix” it in different ways. Most importantly, computers and software that they run have become “smarter”: they have learnt how to turn raw and unconnected data into information, and, eventually, knowledge.

While this data revolution may one day usher in an era of more transparent and accountable governance, Nissenbaum warns that the extreme transparency made possible by the internet may instead undermine the very foundations of a democratic society. To begin with, privacy through obscurity is hardly an option in the age of Google. Second, the tenuous equivalence we have established between “open” and “public” data does not always hold well; that information is in some form available to the public does not automatically dissolve an individual's interest in controlling how it is disseminated. Third, just because the public has a right of access to records does not mean that the public has an automatic right of access to records online; placing them on the internet

often makes those records more public than they ought to be.

Similarly, the aggregation and subsequent dissemination of publicly available information is not as harmless as it seems: a database of banal details does not make a banal database. Plotting someone's DVD rentals against their postal code might disclose just enough to allow an intelligent guess about their identity. A closeted lesbian mother in Ohio is currently suing Netflix, the DVD rental giant, for having disclosed a history of her movie rentals as part of a large data set they released online. This, she argues, could be used to identify her, especially if compared against film reviews she had published on other sites (the suit also urges Netflix not

look through the walls of a house for exactly the same purpose.

Nissenbaum shows that the borders we have drawn between these two domains have been very fuzzy and inconsistent from the very beginning. As our lives become mediated by the internet, the distinction between “private” and “public” becomes even blurrier, revealing the “fault lines that had not before been significant”. This is particularly visible in the workplace: consider companies that have to decide how to deal with employees who use their work computers to post private information to social networking sites. Or how about employees who use corporate pagers to send private text messages? What if they used the corporate pager for private purposes but paid their own fees – do their employers have a right to inspect their correspondence? Such situations are increasingly common in the workplace: a similar case is now facing the US Supreme Court.

To address some of these questions, Nissenbaum proposes a completely new way to think about privacy which transcends the usual paradigms of secrecy and control that have so far dominated the discussion. The framework – which Nissenbaum calls “con-

Some of them are explicitly recognized by law; some – think of etiquette or rules for professional societies, clubs and religious communities – are institutionalized in less formal ways.

Nissenbaum believes that many of our current disagreements about the right to privacy arise because of this variability in interpreting its sources of legitimacy: some want to recognize only the norms that are embedded in law while others opt for a more inclusive definition rooted in custom and tradition. Often, these contexts overlap: a doctor may be inclined to advise a patient to cut out unhealthy food, but as a friend he may also be rather reluctant to take on such a paternalistic attitude. Such conflicts are not a fault of theory; they merely constitute one of the challenges of living within any pluralistic system of values.

Since such norms are usually specific to particular contexts – what is considered appropriate in the context of education may not be so in the context of healthcare – deciding what constitutes a “breach” may require a lengthy investigation of the particular context, the actors involved, the attributes of information and transmission principles. Nissenbaum offers some specific step-by-step guidance on how such an investigation may proceed.

The new framework is not without limitations, which Nissenbaum outlines and addresses as well. Since privacy is only one of the many social goods to strive for, a particular context might demand that the norms be violated. For example, doctors may feel that their contextual integrity is violated as their patients rush to post reviews of their competence online, but this is what the provision of a just and competitive system of healthcare may require.

At the other extreme, it's possible that “contextual integrity” could be used to justify new practices that are already in wide use but have so far escaped the attention of the regulators – what Nissenbaum calls “the tyranny of the novel”. This line of reasoning is, indeed, ubiquitous in the arguments advanced by executives of social networking sites (eg, “we have so many users that like us – what other proof do you need that norms have changed?”).

One way to address such limitations is to identify systemic criteria with which to measure the moral standing of established customs against novel practices. If it's possible to demonstrate the latter's moral superiority, then the violations of contextual integrity can be accepted as morally legitimate. Once again, there are no catch-all solutions here – each context has to be examined on its own merits.

Nissenbaum has written a badly needed and accessible book that can serve as a guide through the emerging digital maze without demanding that we surrender our right to privacy in return. To her credit, she has resisted the temptation to frame her critique in the Foucauldian rhetoric of surveillance and control, grounding most of her arguments in political philosophy and legal theory rather than social theory or cultural studies. Her book offers a straightforward and articulate account of the role that privacy plays in a democratic society, the ways in which technology undermines it, and the steps we need to take to ensure that we don't succumb to the faulty logic of data-hungry corporations.



The camera of a Google Street View car, Hanover, Germany, March 3, 2010

to proceed with their previously announced plans to release an even more refined data set that would contain gender, zipcode, and age information about their users).

To assess the impact of new technologies on privacy, courts have traditionally relied on a poorly defined distinction between “private” and “public” domains. For example, whatever goes on in one's home has been recognized to be off-limits as far as authorities were concerned. In some cases, the courts have extended such protection to places beyond one's house – a telephone booth was found to be a private place that authorities could not wiretap without a proper order. However, no fixed definition emerged of what counts as “private” and “public; in some cases, the courts granted authorities the right to use a helicopter to check a garden for marijuana plants but declined them the right to use heat waves to

textual integrity” – is very ambitious, aiming to provide a normative conception of privacy, to explain our frequent indignation with information technology, and to predict our reaction to its new forms – but she succeeds on all three counts.

To appreciate the intellectual elegance of her argument, one needs to grasp the awkwardly named notion of “context-relative information norms”. What she means by this is that our reaction to information – i.e., whether it makes us angry, irritated or indifferent – depends on the context in which it is transmitted. For example, we don't expect our friends to serve as gossip boards nor do we expect our doctors to discuss our symptoms with other patients. But we probably won't feel offended if something we said in a public meeting was subsequently quoted in the media. Our daily lives are constituted by such contexts and the norms they produce.