November 12, 2010

A Little Less Privacy, a Bit More Security

By SIMON CHESTERMAN

SINGAPORE — The European Union has announced that it will overhaul its data protection rules in 2011. Later this month, the U.S. Federal Trade Commission and Commerce Department will release their own reports on online privacy. Meanwhile, as part of the much-hyped efforts to prepare for “cyberwar,” the U.S. National Security Agency is strengthening ties with organizations like Google and its efforts to mine social networking sites like Facebook.

The dynamic is a familiar one. As usual, privacy will lose.

In recent years, the battleground of privacy has been dominated by fights over warrantless electronic surveillance in the United States and closed-circuit television(CCTV) in Britain. The coming months will see further debates over data mining, DNA databases and biometric identification.

There will be protests and lawsuits, editorials and elections resisting these attacks on privacy. The battles are worthy, but the war will be lost. Efforts to prevent governments from collecting such information are doomed to failure because modern threats increasingly require that governments collect the information; because governments are increasingly able to collect it; and because citizens increasingly accept that they will collect it.

Spying on foreigners has long been regarded as an unseemly but necessary enterprise. Spying on one’s own citizens in a democracy, by contrast, has historically been subject to various forms of legal and political restraint.

There were, to be sure, violations of these principles — spectacularly culminating in Watergate and the resignation of President Richard Nixon. Such scandals reinforced the 20th-century view that foreign and domestic intelligence should and could be kept apart. That position is no longer tenable.

Three factors are driving the erosion of the distinction.

First, many of the threats facing modern democracies do not respect national borders. For the foreseeable future, the most significant threat of violence in countries like the United States will come from terrorists who do not have an obvious state sponsor. The targets of intelligence services will therefore be individuals rather than states.

The second factor is the revolution in technology and communications.

The increased use of electronic communications has been matched by the development of ever more sophisticated tools of

surveillance. It has also blurred the distinction between what is foreign and what is domestic.

The idea that the National Security Agency, for example, can intercept e-mail sent by foreigners but not by U.S. citizens poses — apart from anything else — a technical challenge: When a message is routed through strings of Internet service providers, it is not always clear what is “foreign” and what is “local.”

Third, changes in culture are progressively reducing the sphere of activity that citizens can reasonably expect to be kept from government eyes. This is most obvious in the amount of information voluntarily disclosed through social-networking Web sites, as well as the increased toleration of CCTV in public spaces. It is also implicit in the use of e-mail, credit cards, and other everyday transactions where significant amounts of personal information are passed on to corporations, the government or both.

Arguments over the appropriate balance between liberty and security have a long pedigree. During debates on the U.S.A. Patriot Act in 2001, one senator invoked a founding father: “As Ben Franklin once noted, ‘if we surrender our liberty in the name of security, we shall have neither.’” In fact Franklin’s words were more nuanced: “Those who would give up essential Liberty to purchase a little temporary Safety deserve neither Liberty nor Safety.”

More than two centuries later, the idea that we must choose between liberty and safety needs to be rethought. Instead of simply entrusting governments and other actors with personal data and relying on their good faith, the new arrangement can be thought of as a kind of social contract.

In its traditional formulation, people gave a government coercive powers to make organized society possible. What we are witnessing now is the emergence of a new social contract, in which individuals give the state (and, frequently, other actors) power over information in exchange for security and the conveniences of living in the modern world.

In a post-privacy world, the debate needs to move away from whether information should be collected and focus on how that information can and should be used. Reframing the question in the language of a social contract, mediated by a citizenry that is an active participant rather than passive target, offers a framework to defend freedom without sacrificing liberty.

Simon Chesterman *is professor of law at the National University of Singapore and director of the New York University School of Law Singapore Program. His book “One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty,” will be published in March.*