PRIO
International Peace Research Institute, Oslo
Institutt for fredsforskning

POLICY BRIEF 5/2008

Security After Privacy: The Transformation of Personal Data in the Age of Terror

J. Peter Burgess, *International Peace Research Institute, Oslo (PRIO)*

In the few years since the attacks of 11 September 2001, *security* as a political discourse has grown and evolved more than any other discourse in recent memory

Yet, despite the way it dominates European politics, security has not always been a central concern for Europe. At the moment of its birth, the *threats* faced by the European Community were of an entirely different kind than those we face today. The core issues that marked the first 55 years of European construction were primarily *economic* and thus largely organized by a kind of economic rationality.

It is also essential to recall that the European Union we see today was conceived as a *project of peace*. With the horrors of World War II freshly in mind, Robert Schuman, together with Jean Monnet and with the support of Konrad Adenauer, formulated in 1951 the basic idea that the only sure way to prevent future armed conflict on European soil – and, in particular, between France and Germany – was not to shelter the nations from each other, but rather to *integrate* them. The path to that integration, as we all know, was economic.

The Threat to Europe

In this sense, the most clear historical *threat* to Europe in its early days was its *own* historical divisions. European security politics in the early years of the European construction – if we can speak of such a thing – was formed around the *insecurity* caused by Europe's own internal oppositions, cultural differences and historically shaped animosities. The quest for peace and security was based on a perceived need to overcome these divisions.

Europe's primary security challenge was thus in its early years *its relation to itself*. It was an *internal* challenge, one of the self-knowledge and self-understanding of Europe. European security was a gaze into the mirror – to a great extent, the mirror of history. It was, in a way, a problem of Europe's unease with itself, with its own identity, and with its relationship to its 'others'. This kind of *uncomfortable historical intimacy*, I want to suggest, still guides us today, and is living a new life today.

Europe is under threat. But, *who* or *what* exactly is threatened when Europe is threatened? Is it Europe's critical *infrastructure*, its subways, bridges and railways, the nuclear plants and other buildings, its ships and harbours, the sea-lanes from the oil-exporting Middle East that are in danger? Is it the *people* of Europe who are threatened? Its political leaders? Is it the integrity of the Union, its principles and values that are under fire? Or, do threats concern something else, something more fundamental, something more intimate or human?

In my opinion, this is the question of the day. Yes, Europe may be under threat. But, precisely what does it mean to say that Europe is under threat? The question of the security of Europe profoundly engages the notion of privacy. It concerns the relation of Europe to its intimate self, to its people, to its fears, and to its hopes and aspirations. This is the key to understanding the need for privacy.

Technological and Human Conceptions of Privacy

The most widely accepted analysis of the link between security and privacy builds upon the notion that the two concepts are opposed to each other in a more or less zero-sum logic. *More security,* it is generally said, comes only at the cost of *less privacy,* and vice versa. The axis along which this zero-sum game is played out is *technology*.

Some observers have challenged the assumption that security is played out around the question of technology. This discourse and counter-discourse of technology is often linked to the notion of privacy. European citizens, it is often suggested, enjoy less and less privacy as the march of technological development permits more and more invasion into the private sphere.

However, this hypothesis of privacy challenged by technology is only possible if we begin with a purely *technical* conception of privacy. It advances what we might call the *window blind model* of privacy. According to this model, privacy is the blinds of our living-room window, exposing us through a greater or lesser degree of transparency. The model regards privacy as a question of the technical ability of those who protect or endanger us to *see through* our living-room blinds by technical means, and thus to penetrate our private sphere.

Privacy, according to this technological vision, is a question of borders, of limits, of a clear distinction between the *inside* that is private and the *outside* that is public, between what is entirely *mine* and what is entirely *yours*. It is the distinction between an emotional, moral, spiritual self on the *inside* and a non-emotional, non-moral, non-spiritual environment on the *outside*. It is a conception of privacy guided by rules of inclusion and exclusion, by locked doors, by sealed files and by forbidden knowledge.

This *technological conception of privacy* dominates in European security thinking today. Yet, this conception, built on a link between security, technology and privacy, is problematic for fundamental reasons.

Where does it go wrong, and what are the alternatives to it? Let us begin to answer this question by taking a closer look at the notion of *privacy.*

Privacy

We can analyse the concept of *privacy* in both a *broad sense* and a *narrow sense*.

First, in a broad sense, privacy is one of the most powerful notions in Western cultural history. It organizes a broad spectrum of knowledge and cultural practice, from politics to law, from health to hygiene and sexuality, from family relations to commerce. In particular, it has solid foundations in European philosophical history, reaching back to Aristotle's famous distinction between the *public sphere,* where political activity takes place, and the *private sphere,* where family life takes place.

In its broadest sense, privacy is also a *moral concept.* It involves claims about the moral status of the individual self, about its dignity, and about its relation to others. Philosophers and legal theorists, for example, tend to talk about privacy in terms of ideas like 'inviolate personality'. This moral core, it is argued, is the origin of social values like 'autonomy', 'integrity', 'independence', etc. These values form the foundation of today's notions of human rights, citizenship and civic obligation. They form the foundational core of European civil life.

Closely related to the notion of privacy as inviolate personality is the notion of privacy as *intimacy*. Ideas like love, friendship, loyalty, trust, etc. are only possible in relation to some sort of assurance of privacy. The spheres of experience that support these intimate ideas, all of which are essential to individual moral character, are made possible by a certain understanding of privacy.

Second, in the narrow sense, privacy can be differentiated across three levels.

On one level, *privacy is knowledge*. It is knowledge about the private sphere of a person's life. This links with the broad sense of privacy as moral integrity.

On another level, *privacy is meta-knowledge*. It is knowledge *about* intimate knowledge, about who knows what and where such information came from. Like security itself, privacy thus involves a kind of insight. Privacy is thus information about information.

On yet a third level, *privacy is power over or control of knowledge*. It is control of knowledge *about* information *about* the person whose privacy is in question. It concerns not only information about individuals, but also the right allegedly held by individuals to determine how information about them is used. Thus, relative to the object of privacy – the person – privacy in common discourse is thrice removed.

Privacy at the Heart of Europe

Traditionally, *privacy* lies at the heart of the European self-understanding. It concerns the personhood of the person, the sovereignty of the mind, rationality, will, judgement, taste and spirit. In short, it is the very foundation of the modern European notion of the *citizen,* and thereby of the legitimacy of the European political institutions.

In other words, whatever we may think about the concept of privacy and its relevance today, it is the unique link to the core European principles of law, governance and, not least, science. Despite the

hard times the 18th century conception of the individual has weathered, the European Union, perhaps even more than other institutions, is deeply indebted to it. Among other things, privacy provides the basic support for the Universal Declaration of Human Rights, the European Convention on Human Rights, the various treaties of the European Union and, most recently, the Charter of Fundamental Rights of the European Union.

The Transformation of Privacy

This fundamental concept of privacy has not been a stable one. Indeed, it has changed radically in the last decades. Not surprisingly, changes in the notion of privacy have followed changes in the notion of *information*. Innovation at the meeting place of information technology and human behaviour first erupted onto the European public sphere in the 1980s via commercial marketing practices.

At the centre of this transformation of the classical concept of privacy is a shift in the notion of knowledge of the person in the information age: *personal data*. The emergence of personal data is a key historical event. It represents a kind of shift from *personal* knowledge understood as self-knowledge (which one can only have of oneself) to personal knowledge as knowledge *about* the self (which can be had by another).

European Union legal and ethical responses to this evolution, vaguely understood as a threat, have been robust. This response has taken the form of a number of initiatives ranging from the Convention on Data Protection in 1981 to the way the framework decision on data protection in police and judicial cooperation, passed down last year.

This last development is remarkable, because in some sense it relates precisely to European data legislation and executive order: the use of personal data in the maintenance of *collective* security. Here we see an *extraordinary* parting of ways in European thinking about the relation between privacy and security. The shift encompasses in effect two simultaneous changes.

First, the concept of the *person,* which once lay at the core of the idea of privacy, has become *detached* from knowledge about it, the very knowledge that was to be protected in the name of the person's privacy. While we can still talk of a person's privacy as a kind of relation to knowledge about the person, this knowledge is no longer the sole dominion of that person. The assumption of a right to control knowledge about oneself is no longer reserved to the person. *Information* about the person is no longer *personal*, but rather transportable, commercial, marketable.

Second, this private knowledge, now detached from the person, shifts from being an expression of the *moral particularity* of the person to being the expression of the *person as a threat* to security. Intimate knowledge, the once-protected core of the individual, is now regarded as a kind of codebook for danger. Personal information is the key to revealing the person as a threat. In this way, privacy is no longer a kind of assurance of the integrity of the person, but rather itself a threat to the security of others. *Data protection* thus no longer functions as a protection of the privacy of the person, but rather becomes ongoing innovation in ways to *breach* the privacy of individuals. Privacy is no longer part of the humanity of humans: it is part of the security problem that humans can potentially represent.

Thus, an extraordinary transformation has taken place between the late 1980s, when information technology first began to exert influence on European society, and today, where information, far more than hard security practices, is seen as the key to European security. Privacy has metamorphosed from being *the object of security* to a *very threat to security*. We have moved from a modern society, organized around a legal, economic, social, cultural and moral separation between a private sphere and a public sphere, to a late- or postmodern society where that separation has become the *threat* to society itself.

Biometrics

The key to this tendency is linked to the rise of biometrics, the new technologies being developed for recognizing individuals based on their biological characteristics alone.

The terrorist bombing in Madrid on 11 March 2004 had an acute political impact on Europe and gave momentum to a number of new security policies relevant to biometrics. Among others, these include framework decisions on the fight against terrorism and the European arrest warrant, a strengthening of EU border controls, widened access to communications traffic data, the creation of a European register of criminal convictions, enhanced sharing of passenger name records (PNR), and broadening of the powers of Europol and Eurojust.

What these biometrically oriented policies share in common is that they presuppose that the threat to Europe is an *other,* something *out there, foreign, different* from us, and that it can be adequately *identi-*

fied, isolated, understood and *tracked* through biometric means.

This type of human measure has continued to evolve through changes in the Schengen Information System and the Schengen Visa System. The most recent – and most remarkable – is the recently announced Automated Border Control System (ABCS) and an electronic travel authorization system. The AMCS is a Europe-wide and interlinked border management system that will enable automatic electronic identification of a traveller's *identity*, based on biometric technology.

Enhancing Privacy Through Technology: The Circle Closes

Policymakers in Brussels have *not* gone unaware of this development in the battle over concepts of privacy and security. The European Commission has clearly recognized this slide toward a kind of demonization of the notion of privacy, and has responded by reintroducing and reinscribing a distinction between *good privacy* and *bad privacy.* Already in its communication on a strategy for a secure information society of May 2006, it reaffirmed the need to fulfil already existing data protection rules. In the more recent communication on promoting data protection, the Commission launches a new concept of Privacy Enhancing Technology (PET). It may, however, be an idea to open a discussion about supplementing the notion of Privacy Enhancing Technology (PET) with the notion of Privacy Enhancing Humanity (PEH).

The relation between privacy and security has thus gone the entire circle from privacy as threatened by technology, to privacy as concealed threat that can be discovered through technology, to privacy as advanced by technology.

These reflections lead us to six interrelated conclusions:

1. It will be important in coming years to avoid the technological inertia that leads us to regard the *person* and *personal data* as identical.
2. If there is any place where the *humanity* of people should precede the *European-ness* of people, it is Europe itself.
3. *Technology is not only technical.* It would be far simpler if technology were truly only technical. However, for better or worse, technology is deeply and richly human, and quickly takes on social, cultural and moral dimensions we thought we had escaped through technology.
4. *Security and privacy are not related in a zero-sum trade-off with privacy*. They are deeply dependent upon one another. Security requires privacy, and privacy requires security.
5. We thus need an analysis of the *consequences* of adding *information* to the list of free-flowing quantities in the Schengen Area, that is, to the free flow of people, goods and services.
6. Security research must evoke at all levels the question of *for whom, by whom, in the name of whom* security is assured.

These arguments are *not moral*, but *pragmatic*: Efficient and cost-effective security technology is only possible through attention to the people whom it presupposes and whom it ultimately is intended to serve.

ISBN: 978-82-7288-268-5

PRIO
International Peace Research Institute, Oslo
Institutt for fredsforskning

International Peace Research Institute, Oslo (PRIO)
Hausmanns gate 7
NO 0186 Oslo
Norway
E-mail: info@prio.no
www.prio.no