

The need for global privacy standards

Peter Fleischer, Global Privacy Counsel, Google

Introduction

How should we update privacy concepts for the Information Age? The total amount of data in the world is exploding, and data flows around the globe with the click of mouse. Every time you use a credit card, or every time you use an online service, your data is zipping around the planet. Let's say you live in France and you use a US company's online service. The US company may serve you from any one of its numerous data centers, from the "cloud" as we say in technology circles, in other words, from infrastructure which could be in Belgium or Ireland – and which could change based on momentary traffic flows. The company may store offline disaster recovery tapes in yet another location (without disclosing the location, for security purposes). And the company may engage customer service reps in yet another country, say India. So, your data may move across 6 or 7 countries, even for very routine transactions.

As a consumer, how do you know that your data is protected, wherever it is located? As a business, how do you know which standards of data protection to apply? As governments, how do you ensure that your consumers and your businesses can participate fully in the global digital economy, while ensuring their privacy is protected?

The story illustrates the argument I want to make today. It is that businesses, governments but most of all citizens and consumers would all benefit if we could devise and implement global privacy standards. In an age when billions of people are used to connecting with data around the world at the speed of light, we need to ensure that there are minimum privacy protections around the world. We can do better, when the majority of the world's countries offer virtually no privacy standards to their citizens or to their businesses. And the minority of the world's countries that have privacy regimes follow divergent models. Today, citizens lose out because they are unsure about what rights they have given the patchwork of competing regimes, and the cost of compliance for businesses risks chilling economic activity. Governments often struggle to find any clear internationally recognised standards on which to build their privacy legislation.

Of course there are good reasons for some country-specific privacy legislation. The benefits of homogeneity must be balanced by the rights of legitimate authorities to determine laws within their jurisdictions. We don't expect the same tax rules in every country, say some critics, so why should

we expect the same privacy rules? But in many areas affecting international trade, from copyright to aviation regulations to world health issues, huge benefits have been achieved by the setting of globally respected standards. In today's inter-connected world, no one country and no one national law by itself can address the global issues of copyright or airplane safety or influenza pandemics. It is time that the most globalised and transportable commodity in the world today, data, was given similar treatment.

So today I would like to set out why I think international privacy rules are necessary, and to discuss ideas about how we create universally respected rules. I don't claim to have all the answers to these big questions, but I hope we can contribute to the debate and the awareness of the need to make progress.

Drivers behind the original privacy standards

But first a bit of history. Modern privacy law is a response to historical and technological developments of the second-half of the 20th century. The ability to collect, store and disseminate vast amounts of information about individuals through the use of computers was clearly chilling against the collective memories of the dreadful mass-misuse of information about people that Europe had experienced during WWII. Not surprisingly, therefore, the first data privacy initiatives arose in Europe, and they were primarily aimed at imposing obligations that would protect individuals from unjustified intrusions by the state or large corporations, as reflected in the 1950 European [Convention](#) for the Protection of Rights and Fundamental Freedoms.

Early international instruments

After a decade of uncoordinated legislative activity across Europe, the [Organisation for Economic Co-operation and Development](#) identified a danger: that disparities in national legislations could hamper the free flow of personal data across frontiers. In order to avoid unjustified obstacles to transborder data flows, in 1980 the OECD adopted its [Guidelines](#) on the Protection of Privacy and Transborder Flows of Personal Data. It's worth underscoring that concerns about international data flows were already being addressed in a multinational context as early as 1980, with the awareness that a purely national approach to privacy regulation simply wasn't keeping abreast of technological and business realities.

These OECD Guidelines became particularly influential for the development of data privacy laws in non-European jurisdictions. The Guidelines represent the first codification of the so-called 'fair information principles'. These eight principles were meant to be taken into account by OECD member countries when passing domestic legislation and include: 1) collection limitation, 2) data quality, 3) purpose specification, 4) use limitation, 5) security safeguards, 6) openness, 7) individual participation, and 8) accountability.

A parallel development in the same area but with a slightly different primary aim was the Council of Europe [Convention](#) on the Automated Processing of Personal Data adopted in 1981. The Convention's purpose was to secure individuals' right to privacy with regard to the automatic processing of personal data and was directly inspired by the original European Convention on human rights. The Council of Europe instrument sets out a number of basic principles for data protection, which are similar to the 'fair information principles' of the OECD Guidelines. In addition, the Convention establishes special categories of data, provides additional safeguards for individuals and requires countries to establish sanctions and remedies.

The different origins and aims of both instruments result in rather different approaches to data privacy regulation. For example, whilst the Convention relies heavily on the establishment of a supervisory authority with responsibility for enforcement, the OECD Guidelines rely on court-driven enforcement mechanisms. These disparities have been reflected in the laws of the countries within the sphere of influence of each model. So, for example, in Europe, privacy abuses are regulated by independent, single-purpose bureaucracies, while in the US, privacy abuses can be regulated by many different government and private bodies (e.g., the Federal Trade Commission at the Federal level, Attorneys General at the State levels, and private litigants everywhere). It's impossible to say which model is more effective, since each reflects the unique regulatory and legal cultures of their respective traditions. Globally, we need to focus on advocating privacy standards to countries around the world. But we should defer to each country to decide on its own regulatory models, given its own traditions.

Current situation

Today, a quarter century later, some countries are inspired by the OECD Guidelines, others follow the European approach, and some newer ones incorporate hybrid approaches by cherry-picking elements from existing frameworks, while the significant majority still has no privacy regimes at all.

After half a decade of negotiations, in 1995, the EU adopted the Data Protection [Directive](#) 95/46/EC. The EU Directive has a two-fold aim: to protect the right to privacy of individuals, and to facilitate the free flow of personal data between EU Member States. Despite its harmonisation purpose, according to a recent EU Commission [Communication](#), the Directive has not been properly implemented in some countries yet. This shows the inherent difficulty in trying to roll out a detailed and strict set of principles, obligations and rights across jurisdictions. However, the Commission has also made it clear that at this stage, it does not envisage submitting any legislative proposals to amend the Directive.

In terms of core European standards, the best description of what the EU privacy authorities would regard as "adequate data protection" can be found in the Article 29 Working Party's document [WP 12](#). This document is a useful and detailed point of reference to the essence of European data privacy rules,

comprising both content principles and procedural requirements. In comparison with other international approaches, EU data privacy laws appear restrictive and cumbersome, particularly as a result of the stringent prohibition on transfers of data to [most countries](#) outside the European Union. The EU's formalistic criteria for determining "adequacy" have been widely criticized: why should Argentina be "adequate", but not Japan? As a European citizen, why can companies transfer your data (even without your consent) to Argentina and Bulgaria and other "adequate" countries, but not to the vast majority of the countries of the world, like the US and Japan? In short, if we want to achieve global privacy standards, the European Commission will have to learn to demonstrate more respect for other countries' approach to privacy regimes.

But at least in Europe there is some degree of harmonisation. In contrast, the USA has so far avoided the adoption of an all-encompassing Federal privacy regime. Unlike in Europe, the USA has traditionally made a distinction between the need for privacy-related legislation in respect of the public and the private sectors. Specific laws have been passed to ensure that government and administrative bodies undertake certain obligations in this field. With regard to the use of personal information by private undertakings, the preferred practice has been to work on the basis of sector-specific laws at a Federal level whilst allowing individual states to develop their own legislative approaches. This has led to a flurry of state laws dealing with a whole range of privacy issues, from spam to pretexting. There are now something like 37 different USA State laws requiring security breach notifications to consumers, a patchwork that is hardly ideal for either American consumer confidence or American business compliance.

The complex patchwork of privacy laws in the US has led many people to call for a simplified, uniform and flexible legal framework, and in particular for comprehensive harmonised Federal privacy legislation. To kick start a serious debate on this front, a number of leading US corporations set up in 2006 the Consumer Privacy Legislative [Forum](#), of which Google forms part. It aims to make the case for harmonised legislation. We believe that the same arguments for global privacy standards should also apply to US Federal privacy standards: improve consumer protections and confidence by applying a consistent minimum standard, and ease the burdens on businesses trying to comply with multiple (sometimes conflicting) standards.

A third and increasingly influential approach to privacy legislation has been developing in Canada, particularly since the federal Personal Information Protection and Electronic Documents Act ("[PIPEDA](#)") was adopted in 2000. The Canadian PIPEDA aims to have the flexibility of the OECD Guidelines – on which it is based – whilst providing the rigour of the European approach. In Canada, as in the USA, the law establishes different regimes for the public and private sectors, which allows for a greater focus on each. As has also been happening in the USA in recent years with state laws, provincial laws have recently taken a leading role in developing the Canadian model. Despite the fact that PIPEDA creates a privacy framework that requires the provincial laws to be "substantially similar" to the federal statute, a Parliamentary

Committee carrying out a formal review of the existing framework earlier this year, recommended reforms for PIPEDA to be modelled on provincial laws. Overall, Canada should be praised for encouraging the development of progressive legislation which serves the interests of both citizens and businesses well.

Perhaps the best example of a modern approach to the OECD privacy principles is to be found in the APEC Privacy [Framework](#), which has emerged from the work of the 21 countries of the Asia-Pacific Economic Cooperation forum. The Framework focuses its attention on ensuring practical and consistent privacy protection across a very wide range of economic and political perspectives that include global powerhouses such as the US and China, plus some key players in the privacy world (some old, some new), such as Australia, New Zealand, Korea, Hong Kong and Japan. In addition to being a sort of modern version of the old OECD Guidelines, the Framework suggests that privacy legislation should be primarily aimed at preventing harm to individuals from the wrongful collection and misuse of their information. The proposed framework points out that under the new “preventing harm” principle, any remedial measures should be proportionate to the likelihood and severity of the harm.

Unfortunately, the co-existence of such diverse international approaches to privacy protection has three very damaging consequences: uncertainty for international organisations, unrealistic limits on data flows in conflict with global electronic communications, and ultimately loss of effective privacy protection.

New (interconnected) drivers for global privacy standards

Against this background, we are witnessing a series of new phenomena that evidence the need for global privacy standards much more compellingly than in the 70s, 80s or 90s. The development of communications and technology in the past decade has had a marked economic impact and accelerated what is commonly known as ‘globalisation’. Doing business internationally, exchanging information across borders and providing global services has become the norm in an unprecedented way. This means that many organisations and those within them operate across multiple jurisdictions. The Internet has made this phenomenon real for everyone.

A welcome concomitant of the unprecedented technological power to collect and share all this personal information on a global basis is the increasing recognition of privacy rights. The concept of privacy and data protection regimes has moved from one discussed by experts at learned conferences to an issue that is discussed and debated by ordinary people who are increasingly used to the trade offs between privacy and utility in their daily lives. As citizens’ interest in the issue has grown, so, of course has politicians’ interest. The adoption of new and more sophisticated data privacy laws across the world and the radical legal changes affecting more traditional areas of law show that both law makers and the courts perceive the need to

strengthen the right to privacy. Events which have highlighted the risks attached to the loss or misuse of personal information have led to a continuous demand for greater data security which often translates into more local laws, such as those requiring the [reporting of security breaches](#), and [greater scrutiny](#).

Routes to the development of global privacy standards

The net result is that we have a fragmentation of competing local regimes, at the same time as we the massively increased ability for data to travel globally. Data on the Internet flows around the globe at nearly the speed of light. To be effective, privacy laws need to go global. But for those laws to be observed and effective, a realistic set of standards must emerge. It is absolutely imperative that these standards are aligned to today's commercial realities and political needs, but they must also reflect technological realities. Such standards must be strong and credible but above all, they must be clear and they must workable.

At the moment, there are a number of initiatives that could become the guiding force. As the most recent manifestation of the original OECD privacy principles, one possible route would be to follow the lead of the APEC Privacy Framework and extend its ambit of influence beyond the Asia-Pacific region. One good reason for adopting this route is that it already balances very carefully information privacy with business needs and commercial interests. At the same time, it also accords due recognition to cultural and other diversities that exist within its member economies.

One distinctive example of an attempt to rally the UN and the world's leaders behind the adoption of legal instruments of data protection and privacy according to basic principles is the Montreux [Declaration](#) of 2005. This Declaration probably represents the first official written attempt to encourage every government in the world to do something like this and this is an ambition that must be praised. Little further was heard about the progress of the Montreux Declaration until the International Privacy Commissioners' Conference took place in November 2006 and the London [initiative](#) was presented. The London Initiative acknowledged that the global challenges that threaten individuals' privacy rights require a global solution. It focuses on the role of the Commissioners' Conference to spearhead the necessary actions at an international level. The international privacy commissioners behind the London Initiative argue that concrete suggestions must emerge in order to accomplish international initiatives, harmonise global practices and adopt common positions.

One privacy commissioner who has expressed great interest in taking an international role aimed developing global standards is the UK Information Commissioner. The Data Protection [Strategy](#) of the Information Commissioner's Office published at the end of June 2007 stresses the importance of improving the image, relevance and effectiveness of data protection worldwide and, crucially, recognises the need for simplification.

Way forward

The key priority now should be to build awareness of the need for global privacy standards. Highlighting and understanding the drivers behind this need – globalisation, technological development, and emerging threats to privacy rights – will help policymakers better understand the crucial challenge we face and how best to find solutions to address them.

The ultimate goal should be to create minimum standards of privacy protection that meet the expectations and demands of consumers, businesses and governments. Such standards should be relevant today yet flexible enough to meet the needs of an ever changing world. Such standards must also respect the value of privacy as an innate dimension of the individual. To my mind, the APEC Framework is the most promising foundation on which to build, especially since competing models are flawed (the USA model is too complex and too much of a patchwork, the EU model is too bureaucratic and inflexible).

As with all goals, we must devise a plan to achieve it. Determining the appropriate international forum for such standards would be an important first step, and this is a choice that belongs in the hands of many different stakeholders. It may be the OECD or the Council of Europe. It may be the International Chamber of Commerce or the World Economic Forum. It may be the International Commissioners' Conference or it may be UNESCO. Whatever the right forum is, we should work together to devise a set of standards that reflects the needs of a truly globalised world. That gives each citizen certainty about the rules affecting their data, and the ability to manage their privacy according to their needs. That gives businesses the ability to work within one framework rather than dozens. And that gives governments clear direction about internationally recognised standards, and how they should be applied.

Data is flowing across the Internet and across the globe. That's the reality. The early initiatives to create global privacy standards have become more urgent and more necessary than ever. We must face the challenge together.