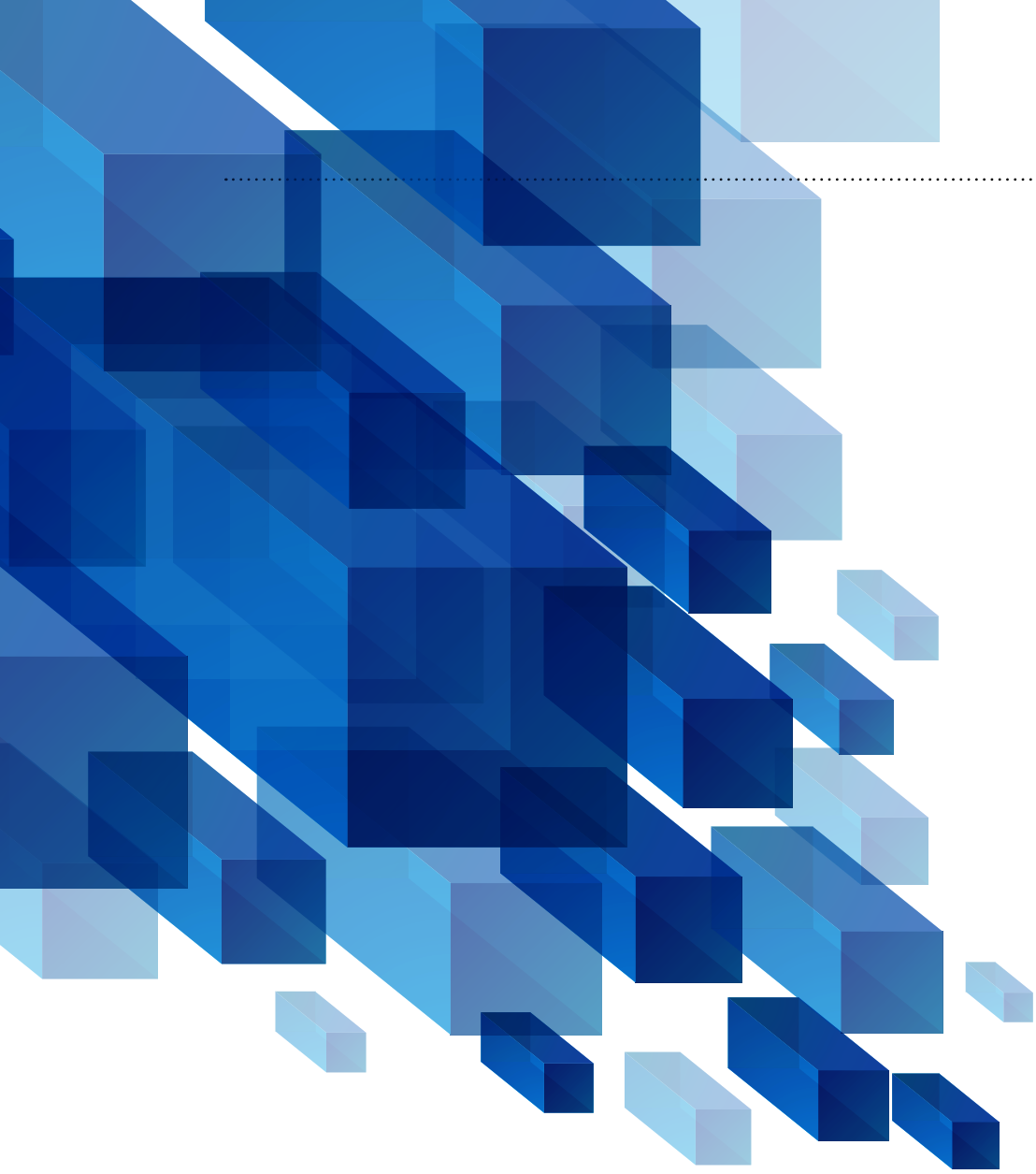


December 2013

Data Protection Principles for the 21st Century

Revising the 1980 OECD Guidelines

Fred H. Cate
Distinguished Professor and C. Ben Dutton Professor of Law,
Maurer School of Law, Indiana University

Peter Cullen
General Manager, Trustworthy Computing Governance,
Microsoft Corporation

Viktor Mayer-Schönberger
Professor of Internet Governance and Regulation,
Oxford Internet Institute, University of Oxford

Contents

Foreword 2

Acknowledgments 4

Introduction 5

The OECD Guidelines in a Changing World 6

The Path to Revising the Guidelines 8

Revising the OECD Guidelines 10

Introducing the Revised Guidelines 11

The Revised Principles 13

Appendix 22

Foreword

Since their publication by the Organisation for Economic Co-operation and Development (OECD) more than 30 years ago, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data have influenced those who have tried to strike an appropriate balance between data use and the protection of personal privacy. While the 1980 OECD Guidelines were not the earliest articulation of fair information principles, they have been uniquely successful—in large part because they were created and endorsed by a group of renowned international experts representing many of the world's major economies. Over the years, they have become the foundation for most national laws governing data protection.

The OECD Guidelines took a comprehensive approach, covering data collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The world was of course a very different place when the Guidelines were adopted. The principles laid out in the Guidelines were crafted for a simpler time when data types and use were less complex; organizations collected data from individuals, stored that data in a computer, and then made deterministic uses and decisions about the individual based on that data.

The Guidelines were a response to the concern, even in those days of relatively simple data collection and use, that individuals would lose their right to information privacy—that is, they would lose the right to decide for themselves how their data would be used, who it would be shared with, and for what purposes. In light of that overarching concern, the principles relating to purpose specification, use limitation, and consent of the data subject were viewed as particularly important, and it became commonplace to provide privacy notices and seek user consent for data collection and use. This approach worked, at least where appropriate, because only large organizations had the resources to manage mainframe computers and most data relationships were binary ones involving the data user (and its agents) and the data subject.

If there was a "canary in the coal mine," it was the now famous (or some would say infamous) statement by Scott McNealy, then-CEO of Sun Microsystems, that "you have zero privacy anyway…. Get over it."[1] The statement was prompted by a dramatically changing world, with trends that continue to this day. The amount of data has been increasing not incrementally but exponentially. New forms of data have emerged, such as user-generated content, observed data, genetic information, and GPS data—to name but a few. New forms of sharing have developed, from social networking to machine-to-machine transactions in which data is shared without active human involvement. New innovations have generated important insights from existing data, such as when DNA from old blood samples clears the innocent

[1] See the whitepaper titled "Trustworthy Computing Next" by Scott Charney at www.microsoft.com/en-us/download/details.aspx?id=29084.

or when sophisticated algorithms used on previously collected personal information results in medical breakthroughs that save lives. In some of these cases, the subsequent value of the data analyzed has not been clear at the time of collection or creation.

Balancing the competing interests of data protection and data use in this new world involves addressing new challenges. This is why the revised data protection principles presented in this paper are so important. If the goals that informed the 1980 OECD Guidelines are to have meaning in the 21st century, we must ensure that fair information principles can still be applied effectively. It will not be enough to hold on to old paradigms, such as heavy reliance on notice and choice—at least not when the average person could spend a month every year reading privacy statements.

Individual participation will remain important, but the question that vexes us now is the same one that confronted the OECD in an earlier age: How can we ensure data protection while enabling the personal and societal benefits that come from the use of data? Achieving both objectives in our connected age will require new thinking and, perhaps, amended principles. Above all, we need to have a robust discussion and build consensus soon, before we are overtaken by events.

Scott Charney
Corporate Vice President
Trustworthy Computing Group
Microsoft Corporation

Acknowledgments

The proposed revisions in this document were developed by a working group organized by the Oxford Internet Institute (OII), University of Oxford. The organizers thank the members of the working group, who gave generously of their time and expertise:

Fred H. Cate, Moderator
Distinguished Professor and C. Ben Dutton Professor of Law,
Maurer School of Law, Indiana University
Director, Center for Applied Cybersecurity Research

Peter Cullen
General Manager, Trustworthy Computing Governance,
Microsoft Corporation

Philip Evans
Senior Partner and Managing Director of the Boston Office,
Boston Consulting Group

Yoram Hacohen
Former Head,
Israeli Law, Information, and Technology Authority (ILITA)

Viktor Mayer-Schönberger, Moderator
Professor of Internet Governance and Regulation,
Oxford Internet Institute, University of Oxford

Yann Padova
Senior Counsel, Baker McKenzie;
Former Secretary General,
French Commission Nationale Informatique et Libertés (CNIL)

Richard Thomas, CBE
Former Information Commissioner of the United Kingdom

The authors also gratefully acknowledge the excellent research assistance of Amanda Craig.

Introduction

In the 1970s, as computers were increasingly used to process and transfer personal data, European and North American countries began enacting information privacy laws. As they did so, concerns quickly emerged about the extent to which inconsistencies among such laws might disrupt the increasingly global flow of information. To facilitate interoperability, the Organisation for Economic Co-operation and Development (OECD) published the first international information privacy guidelines in 1980.[2]

Today, the OECD Guidelines form the basis of most information privacy legislation around the world. In an attempt to balance the "fundamental but competing values" of "privacy and the free flow of information," they establish minimum standards for protecting personal data. Their central requirement is that the collection and use of personal data be both limited and lawful—that is, either explicitly permitted by law or consented to by individuals to whom the data pertains, as well as limited to the minimum collection and use necessary to achieve the stated purpose and not used for other, unrelated purposes. The Guidelines also require that personal data be secured, reasonably accessible, and managed openly and with accountability.

In the 33 years since, our interaction with computers has vastly expanded in terms of both global scale and individual use. The Domain Name System was implemented, and IPv4 address allocation was exhausted. At-home desktop computers were popularized and have since been supplemented and increasingly replaced by mobile technology. The World Wide Web, Google, Bing, Twitter, and Facebook were invented, and the Internet has become a global commercial and social medium.

As a result, the amount and variety of personal data generated and processed through computers have expanded beyond what most people could have imagined in 1980. Many of us read the news, check blogs, socialize with friends, communicate with co-workers and other communities, conduct banking transactions, do research, shop, listen to music, watch videos, and do many other activities online every day—through our computers, smart phones, or tablets.

This vast increase in online interactions and information sharing has had compounding effects. For one, user expectations have shifted. Such pervasive daily computer and Internet use means that lack of regular access to these resources can be a serious inconvenience, if not a serious impediment. In addition, businesses and governments have many more opportunities to collect personal information about individuals and their online habits.

[2] Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Meanwhile, data storage has become relatively inexpensive and data analytics have become more sophisticated. We have arrived at the age of "Big Data." Massive, rich data sets are collected and analyzed to advance progress in fields as wide-ranging as public health, political science, law enforcement, personal relationships, consumer behavior, national security, sports, weather, and manufacturing. International Data Corporation (IDC), a leading technology market research firm, estimates that the amount of data in the world doubles every two years.[3]

In short, all of the aforementioned factors have contributed to rethinking the original Guidelines that formed the basis of most information protection frameworks and most privacy legislation around the world.

The OECD Guidelines in a Changing World

The world of Big Data poses serious information privacy risks that are exacerbated by the "notice and consent" requirements in the 1980 Guidelines and reflected in most modern data protection laws. In most cases, the collection of personal data not only requires the consent of the data subject but is also limited to the minimum amount of data necessary to achieve the purpose identified in the notice used to solicit consent, and that data may not be used for other, unrelated purposes without new consent. While this approach may have been feasible in 1980, it does little to protect individuals today or support the valuable new uses of personal data.

In 1980, the burden on individuals to read and understand privacy policies was more tolerable because online interactions were less frequent and there were far fewer data collectors and data users. Businesses and governments were also using personal data in more straightforward ways, often for a single, well-defined purpose, and not sharing it with numerous third parties and developing complex data sets. Under these circumstances, individuals were more likely to understand the purpose for which their data was being collected and used. And ultimately they could be held accountable for supplying informed consent when given adequate notice.

Even now, this approach might seem desirable because it empowers individuals to weigh their own interests in protecting privacy and accessing resources. However, with the proliferation of new information technologies, applications, and data uses, individual consent is rarely exercised as a meaningful choice. Individuals are overwhelmed with many long, complex online privacy policies just as they are

[3] Steve Lohr, "The Age of Big Data," New York Times, Feb. 11, 2012, www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all&_r=0.

attempting to access a desired resource. Many of us have clicked through so many policies that it has become a meaningless process of scrolling and clicking "I agree."

Moreover, even if individuals wished to read the endless privacy policies they encounter, actually doing so would be impossible because of society's growing reliance on personal data. One 2008 study calculated that reading the privacy policies of just the most popular websites would take an individual 244 hours—or more than 30 full working days—each year.[4] In addition, a meaningful assessment of even a single privacy policy would require a sophisticated understanding of how data is used today. This would mean investing even more time to stay current on how data collection and data use are evolving.

Many people do not read privacy policies for the simple reason that those policies stand between them and the service they seek to use. Privacy policies generally do not give individuals the chance to choose among varying degrees of disclosure or third-party use of their data. Rather, individuals must either consent to the privacy policy or abandon use of the service they are attempting to access. Our increasing reliance on many online services means that so-called choice does not present any real options.

More troubling is the broader impact of the heavy reliance on notice and choice. The narrower the scope of notice and consent, the greater the restrictions imposed on future, often unknown uses of data. This can interfere with future benefits and hinder valuable new discoveries. On the other hand, because privacy notices under the 1980 Guidelines constrain future data uses, notices have become increasingly broad and permissive. The result has been the increasing erosion of information privacy. In both cases, the reliance on notice and choice has had the effect of shifting much of the responsibility for data protection away from data collectors and data users and onto data subjects.

In summary, the notice and consent system, on which data collectors and data users have come to rely, was designed to empower individuals to make decisions about their personal data, but the evolution of data collection and data use has severely weakened that power while imposing increasing burdens on data subjects and on society. While notice and consent may provide meaningful privacy protection in appropriate contexts, this approach is increasingly ineffective as the primary mechanism for ensuring information privacy.

In addition, the advent of Big Data and new analytical tools has shown us that many valuable and innovative uses of data are not known at the time of collection. Data collected for one purpose can often be

[4] Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," I/S: A Journal of Law and Policy for the Information Society (2008), http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf.

repurposed in ways that greatly benefit society. The myriad examples include examining health records and lab results for medical research, analyzing billions of Internet search records to map flu outbreaks and identify dangerous drug interactions, searching financial records to detect and prevent money laundering, and tracking vehicles and pedestrians to aid in infrastructure planning. Individuals, businesses, and societies benefit enormously from creative uses of existing data. And yet these uses can also raise serious privacy issues and should therefore be subject to responsible data protection laws.

The Path to Revising the Guidelines

As a practical matter, the evolution of data collection and data use necessitates an evolving system of information privacy protection. A revised approach should shift responsibility away from individuals and toward data collectors and data users, who should be held accountable for how they manage data rather than whether they obtain individual consent. In addition, a revised approach should focus more on data use than on data collection because the context in which personal information will be used and the value it will hold are often unclear at the time of collection.

These have been among the key conclusions of a number of initiatives in recent years to reexamine data protection. While the critique of notice and choice as the primary mechanism for data protection originated with academics—in 1999, Professor Paul Schwartz argued that "social and legal norms about privacy promise too much, namely data control, and deliver too little"[5] —it is increasingly reflected in reviews of existing laws conducted by regulators, industry officials, and privacy advocates. For example, the U.S. Federal Trade Commission noted the dangers of over-reliance on notice and choice in its staff and commission reports (issued in 2010 and 2012, respectively) on the future of privacy protection.[6] In its 2010 staff report, for example, the Commission wrote:

> In recent years, the limitations of the notice-and-choice model have become increasingly apparent..... [C]onsumers face a substantial burden in reading and understanding privacy policies and exercising the limited choices offered to them.... Additionally, the emphasis on notice and choice alone has not sufficiently accounted for other widely recognized fair information practices, such as access, collection limitation, purpose specification, and assuring data quality and integrity.[7]

[5] Paul M. Schwartz, "Privacy and Democracy in Cyberspace," 52 *Vanderbilt Law Review* 1607, 1657 (1999).
[6] U.S. Federal Trade Commission, P*rotecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* FTC Report (2012), www.ftc.gov/os/2012/03/120326privacyreport.pdf; U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,* Preliminary FTC Staff Report (2010), www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[7] Preliminary FTC Staff Report (2010), 19-20.

On December 1, 2009, the EU Article 29 Data Protection Working Party and the Working Party on Police and Justice adopted a "joint contribution" on the future of privacy, in which they argued that "consent is an inappropriate ground for processing" in the "many cases in which consent cannot be given freely, especially when there is a clear unbalance between the data subject and the data controller (for example in the employment context or when personal data must be provided to public authorities)."[8]

In healthcare, a U.S. Institute of Medicine committee of experts adopted a report in 2009 recommending moving beyond notice and choice as the basic protection for health information.[9] A year earlier, former UK Information Commissioner Richard Thomas and Wellcome Trust Director Mark Walport prepared a report at the request of the British prime minister in which they recommended moving beyond individual choice at the time of collection as the basis for British health privacy law."[10]

The World Economic Forum is now in the midst of a multiyear initiative, called "Rethinking Personal Data," that is based on the conviction that "the basic data protection principles…do not work in today's world…. In particular, notice and consent [are] not delivering real effective choice to individuals."[11]

Parallel with these developments, in 2012 Microsoft embarked on a year-long global discussion of data protection. It began with a series of regional privacy dialogues in Washington, D.C.; Brussels; Singapore; Sydney; and São Paulo that Microsoft sponsored between May and August 2012. These events provided an opportunity for small groups of leading regulators, industry executives, public interest advocates, and academic experts to talk frankly about the role of individual control and notice and consent in data protection. The groups also discussed alternative models that might better protect both information privacy and valuable data flows in the emerging world of Big Data and cloud computing.[12]

Following the five regional events, Microsoft invited more than 70 privacy and data protection experts from government, industry, nonprofit organizations, and academia to a global privacy summit in Redmond, Washington, in September 2012. Drawn from 19 countries on five continents, the participants came together to consider the future of data sources and data uses and practical steps to enhance privacy protection.

[8] Article 29 Data Protection Working Party and the Working Party on Police and Justice, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data* (02356/09/EN, WP 168) 17 (Dec. 1, 2009), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf.
[9] Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research* (2009).
[10] Richard Thomas and Mark Walport, *Data Sharing Review Report 70* (2008). *See also* Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research 6* (2009).
[11] World Economic Forum, *Unlocking the Economic Value of Personal Data: Balancing Growth and Protection* (2012), www3.weforum.org/docs/WEF_IT_UnlockingValueData_BalancingGrowthProtection_SessionSummary.pdf; *see also* www.weforum.org/issues/rethinking-personal-data.
[12] For more information and a list of participants at each event, see Fred H. Cate and Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data: Microsoft Global Privacy Summit Summary Report and Outcomes* (Nov. 2012), www.microsoft.com/en-us/download/confirmation.aspx?id=35596.

While the discussions at the regional dialogues and the global summit were wide ranging, a handful of themes emerged with surprising consistency. Foremost among them were the following priorities for modernizing the OECD Guidelines:

- Reduce the focus on data collection and the attending notice and consent requirements, and focus more on a practical assessment of the benefits and risks associated with data uses.

- Eliminate or substantially reduce the role of the Purpose Specification and Use Limitation principles, which require a specific, articulated purpose for collecting personal data and restrict data uses to that purpose or related, "not incompatible" purposes.

- Restore the balance between privacy and the free flow of information that was the original goal of the OECD Guidelines, and avoid suppressing innovation with overly restrictive or inflexible data privacy laws.

- Make data users more accountable for the personal data they access, store, and use, and hold them liable when harm to data subjects occurs.

- Adopt a broader definition of the "harms" that inappropriate uses of personal data can cause, and put in place practical frameworks and processes for identifying, balancing, and mitigating those harms.

Revising the OECD Guidelines

Presented with these recommendations, Microsoft asked the Oxford Internet Institute to organize a small working group of senior leaders with experience in data protection regulation to review the 1980 OECD Guidelines and consider specific revisions to update them for the 21st century.

The working group was moderated by Viktor Mayer-Schönberger, Professor of Internet Governance and Regulation at the University of Oxford and the author of numerous works on data protection, including a new book with *Economist* editor Kenneth Cukier titled *Big Data: A Revolution That Will Transform How We Live, Work, and Think;* and Fred H. Cate, Distinguished Professor and C. Ben Dutton Professor of Law at Indiana University's Maurer School of Law, Director of the Center for Applied Cybersecurity Research, and Co-Director of the Center for Law, Ethics, and Applied Research in Health Information.

The other working group participants were:

Peter Cullen
General Manager, Trustworthy Computing Governance, Microsoft Corporation

Philip Evans
Senior Partner and Managing Director of the Boston Office, Boston Consulting Group

Yoram Hacohen
Former Head, Israeli Law, Information, and Technology Authority (ILITA)

Yann Padova
Senior Counsel, Baker McKenzie
Former Secretary General, French Commission Nationale Informatique et Libertés (CNIL)

Richard Thomas, CBE
Former Information Commissioner of the United Kingdom

The members were selected for their individual expertise and extensive experience; they did not participate as representatives of any institutions with which they were or had been affiliated, and they were not compensated for their participation.

The working group met outside London in January 2013 for intensive discussions and then circulated draft revisions by email throughout the winter and spring. The revisions recommended in this document reflect the consensus view of the working group as a whole, but this does not mean that every member of the working group supported every revision detailed below.

Introducing the Revised Guidelines

The revisions to the OECD Guidelines include basic changes that are essential for the protection of individual privacy in the 21st century, while avoiding unnecessary restrictions on uses of personal information that are increasingly important to individuals, societies, and economies.

To shift responsibility for data protection away from individuals, and to focus on data use rather than data collection, the revised principles make a significant distinction between principles that apply to data collection and those that apply to data use or other processing activities. The chart that accompanies the revised principles helps clarify these important distinctions.

In addition, "use" is defined very broadly, and the Use Principle (formerly the Use Specification Principle) has been greatly expanded. In determining whether certain data uses should be permitted, it requires balancing the harms and benefits of data uses along with measures that are in place to guard against potential harms. In effect, this principle returns to the original OECD goal of balancing the "fundamental but competing values" of "privacy and the free flow of information," but in the context of Big Data. The revised principles, which acknowledge the value of Big Data, apply only to personal data that has not been "deidentified."

Notice and consent still have a place in the revised principles. For example, the Collection Principle (a revision of the Collection Limitation Principle) requires data collectors to evaluate whether individuals might reasonably anticipate that their data will be collected in determining whether consent is required. In addition, the revised principles treat individual choice as a "heightened protection" against potentially harmful data uses, but such choice should be "meaningful" and "clear" as well as "accompanied by relevant, understandable information about the choice and its consequences."

Because personal data is now routinely collected in many more situations and by many more organizations than were even possible in 1980, and risks are heightened in certain contexts, the revised principles are also more context sensitive. Encouraging the weighing of harms, benefits, and measures to mitigate harm means that unique circumstances should be given consideration. In addition, the principles address data collection by government entities separately and require "clear and understandable notice" when personal data "affecting the employment, health care, financial products or services, or legally protected rights of an individual" is involved.

Three final observations are in order. First, the revised data principles represent significant continuity with the 1980 Guidelines.[13] Balancing individual privacy and the flow and use of data remains a central goal. In numerous instances, including the Openness and Security Safeguards principles, added language updates or clarifies the principle rather than alters its substance. Likewise, the Accountability Principle is expanded so regulators can ensure that data processors are adhering to the revised principles. The working group did not make any recommendations that the members did not consider necessary.

Second, it is important to remember that these revised principles, like the 1980 Guidelines, are only principles—they are intended to guide the creation, adoption, and implementation of national laws. Those laws will provide the many details that are necessarily missing from the principles themselves.

[13] See the Appendix for the full text of the 1980 OECD Guidelines, which are included to facilitate comparison.

Third, the working group anticipates that data protection laws may differ significantly from nation to nation, reflecting each country's distinct cultural experiences, as has been the case under the 1980 Guidelines. Consistency with the principles is crucial to ensuring interoperable data protection regimes that meet the needs of increasingly global travel, trade, commerce, education, entertainment, and communications. But achieving more—such as uniformity among the laws—is not only unachievable but also undesirable, given the significant cultural differences.

The revised principles are presented below. The commentary in italics is intended to clarify specific issues and add further explanation; it is not part of the principles themselves.

The Revised Principles

Definitions

Collection. The recording or other collection of personal data.

Data steward. Any person or entity that processes personal data or on whose behalf personal data is processed.

Commentary: The term "data steward" includes both "processors" and "controllers," as defined in the EU Data Protection Directive.

Data user. Any person or entity that uses personal data or on whose behalf personal data is used.

Commentary: The term "data user" is a subset of "data stewards."

Deidentified data. Personal data from which identifying characteristics have been removed or obscured so that it is not reasonably likely that the data could identify an individual. The determination as to which data is deidentified should take into account: (a) the methods, technologies, and other tools used to remove or obscure identifying characteristics, and the possibilities and effort necessary to reidentify particular data; (b) the existence of legal requirements or contractual or other binding undertakings not to reidentify the data; and (c) the sensitivity of the personal data and potential impact to the individual if the data is inappropriately reidentified.

Harm. Includes tangible and material harm (such as physical injury and financial loss), intangible or moral harm (such as damage to reputation or goodwill, or excessive intrusion into private life), and broader societal harm (such as contravention of national and multinational human rights instruments), as defined or determined by applicable law. Harm does not include the rational and reasonable impact of accurate, relevant data appropriately applied to an individual.

Individual. A natural person.

Personal data. Any information that identifies an individual, could reasonably be used to identify an individual, or is linked to data identifying an individual and used in any manner affecting that individual. It does not include deidentified data, except for deidentified data that is linked to data identifying an individual and used in any manner affecting that individual.

Processing. Includes the collection, use, storage, transfer, disclosure, and destruction of personal data.

Use. Relying on or consulting personal data for decision making or other assessment concerning an individual, using personal data to create or infer other personal data, or disclosing or disseminating personal data to a third party. Use does not include collection, storage, or destruction of personal data.

Commentary: "Use" is a subset of "processing" and is defined very broadly.

<table>
<tr><td rowspan="2">Data Activity</td><td colspan="3">Processing</td></tr>
<tr><td>Collection</td><td>Use
(including relying on or consulting personal data for decision making or other assessment concerning an individual, using personal data to create or infer other personal data, and disclosing or disseminating personal data to a third party)</td><td>Other Processing
(including storage and destruction)</td></tr>
<tr><td rowspan="8">Principle</td><td>Collection Principle; Special Principle for Government Collection</td><td></td><td></td></tr>
<tr><td></td><td>Use Principle</td><td></td></tr>
<tr><td></td><td>Data Quality Principle</td><td></td></tr>
<tr><td></td><td>Individual Participation Principle</td><td></td></tr>
<tr><td colspan="3">Openness Principle</td></tr>
<tr><td colspan="3">Security Safeguards Principle</td></tr>
<tr><td colspan="3">Accountability Principle</td></tr>
<tr><td colspan="3">Enforcement Principle</td></tr>
</table>

Principle Applicable to the Collection of Personal Data

1. Collection Principle

a. Personal data should not be collected:

i. in violation of restrictions imposed by law;

ii. through deception; or

iii. in ways that are not apparent to or reasonably discernible by and not reasonably anticipated by the individual.

b. In addition to the requirements of paragraph (1)(a), a governmental entity should not collect data:

i. outside the scope of its legal authority; or

ii. without a legitimate purpose.

Commentary: The Collection Principle, which replaces the Collection Limitation Principle in the 1980 Guidelines, reflects a deliberate effort to move the focus of data protection away from data collection and the attending disclosure and consent requirements. The reasons for this include the following:

- *Data stewards almost always have a legitimate reason for collecting or disclosing personal and identifiable data, so focusing on data collection here often results in marginalizing that protection.*

- *The proliferation of digital information technologies and sensors has led to the increased collection of personal data without the knowledge or awareness of individuals.*

- *The problems associated with making consent meaningful and practical are widespread and well documented.*

- *As more data is collected and storage and transmission costs are reduced, societies are discovering more valuable uses of personal data that were not anticipated at the time of collection.*

- *The existing focus on notice and consent has tended to shift responsibility for data protection to the data subject; moving away from a focus on data collection and the related notice and consent requirements can shift responsibility for data protection to data users.*

The Collection Principle includes compliance with other legal restrictions on collection (for example, laws prohibiting trespassing or harassing), not collecting personal data through deception or fraud, and ensuring transparency by avoiding hidden, unanticipated data collection.

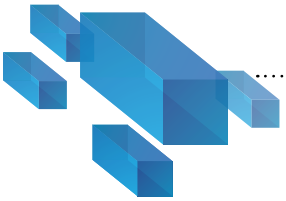
This is the only principle that specifically addresses government activity. It reflects the conviction that, in addition to the provisions applicable to all data collection, government data collection should require general legal authority and a legitimate purpose.

Principles Applicable to the Use of Personal Data

2. Use Principle

a. The permissibility of uses of personal data should be determined by balancing:
   i. the degree and likelihood of benefits resulting from such uses;
   ii. the degree and likelihood of harm posed by such uses; and
   iii. the measures in place to guard against such harm.

b. Uses of personal data reasonably likely to result in:
   i. no or minimal harm to an individual should be permitted with the basic protections required by these Principles;



   ii. significant harm such as physical injury or loss of life should be prohibited; and
   iii. other harms should be permitted with protections in place appropriate to the risk and degree of harm.

c. Individual choice should be required as a protection only if meaningful, and if required should be:
   i. clear;
   ii. used to provide real choice; and
   iii. accompanied by relevant, understandable information about the choice and its consequences.

d. Given the importance of privacy and the flow of personal data, each nation should undertake through a transparent process to determine clearly how harms and benefits are to be evaluated; those uses of personal data which are to be permitted, prohibited, or permitted only with appropriate protections in place; and in what settings or conditions individual consent is an appropriate protection. Nations are encouraged to cooperate in making these determinations and to coordinate their legislative measures.

Commentary: The Use Principle requires data stewards to make a careful assessment of the benefits, harms, and harm mitigation tools in place for each intended data use. The nature of that assessment and the determination of harms (and also perhaps of benefits) may differ from country to country, but the Use Principle encourages predictability and efficiency through the adoption of benchmarks, frameworks, or models and specific categories and/or definitions of harms and benefits. This principle also encourages national governments to cooperate in arriving at these definitions and in coordinating legal implementation.

In the Definitions section, "harm" has a broad meaning that includes tangible and material harm (such as physical injury and financial loss), intangible or moral harm (such as damage to reputation or goodwill, or excessive intrusion into private life), and broader societal harm (such as contravention of national and multinational human rights instruments). Nations should adopt definitions and/or categories of harms that are appropriate to their own setting, and they should ensure that those definitions are widely available.

The term "benefits" is also used broadly here. While the precise determination of what constitutes a benefit may differ depending on national context, the term is meant to include benefits to individuals, data stewards, and society.

The Use Principle anticipates that some uses of data will be routinely permitted (for example, to ensure the security of data) without special or extraordinary data protection tools. Some uses of data may be prohibited outright or may require extraordinary protections. And other—perhaps most—uses will require a context-specific risk assessment and appropriate data protection tools.

This principle acknowledges that individual choice may be one of those appropriate tools, but only if that choice would be meaningful (for example, informed, actionable, and not subject to excessive disparities of bargaining power). Further, when notice and consent is required, it should be clear, provide real choice (not routinely used in take-it-or-leave-it situations), and be accompanied by relevant, understandable information about the choice and its consequences. (The use of the word "choice" here and throughout this paper includes the concept of "consent"; "choice" is used alone simply to avoid the awkward construction of "choice/consent.")

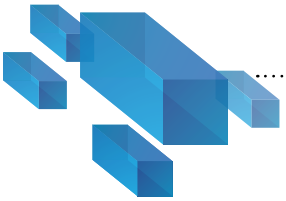
3. Data Quality Principle—Personal data used for a decision affecting individuals should be relevant to the purposes for which they are used and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date.

Commentary: The revised Data Quality Principle is almost identical to the 1980 version except that it applies only to "personal data used for a decision affecting individuals." This limiting phrase is designed to avoid the wasting of resources in trying to assess the accuracy, completeness, and timeliness of data that is not being used in any way that could affect individuals. Moreover, the principle explicitly recognizes that determining accuracy, completeness, and timeliness of data requires knowing for what purpose the data is to be used.

4. Individual Participation Principle

a. A data user that uses personal data in any manner affecting the education, employment, physical or mental health, financial position, or legally protected rights of an individual should provide notice to the individual that personal data is being used, and should make readily available to the individual, without charge, a clear and understandable description of:
   i. the types of personal data used;
   ii. the sources of personal data used;
   iii. how those personal data were or will be used; and
   iv. the individual's legal rights under this Principle.

b. An individual should have the right with regard to personal data used in any manner affecting the education, employment, physical or mental health, financial position, or legally protected rights of that individual to:
   i. obtain access to such personal data relating to the individual within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to the individual;
   ii. challenge the processing and accuracy of personal data relating to the individual and, if the challenge is successful, to have the data erased, rectified, completed, or amended; and
   iii. be given reasons if a request made under subparagraphs (i) and (ii) is denied, and to be able to challenge such denial.



c. A data steward should, upon request, correct inaccurate personal data or provide legitimate reasons for its failure to do so.

Commentary: The revised Individual Participation Principle is stronger than the 1980 version but is limited to situations in which personal data is being used "in any manner affecting the education, employment, physical or mental health, financial position, or legally protected rights of an individual." In these situations, individuals are entitled to: notice that personal data is being used and that the individual can readily obtain information about the intended use; access to the data; the opportunity to challenge the processing and the accuracy of the data; an explanation if either access or correction is not provided or the processing is not stopped; and an opportunity to legally challenge those reasons. These access rights are in addition to any other rights to access personal data that might be provided in other laws, such as laws applicable to employment or consumer protection.

In addition, in all settings, irrespective of the data being used, a data steward has an obligation to correct inaccurate data or "provide legitimate reasons for its failure to do so." "Legitimate reasons" will have to be defined under applicable law and will likely differ from nation to nation, but they could include factors such as errors that pose no risk of harm to data subjects, especially if those errors are expensive or unduly burdensome to correct.

In addition to this Individual Participation principle, individuals of course retain their right to rescind consent in all cases in which they explicitly consented to the processing of personal data as part of a notice and choice mechanism.

Principles Applicable to the Collection, Use, or Other Processing of Personal Data

5. Openness Principle—There should be a policy of openness about practices and policies with respect to the processing of personal data.
   a. Means should be readily available for establishing in general terms the existence of personal data processing, the nature of personal data being processed, how such data is protected, and, if applicable, the major purposes for which it is used.
   b. The identity, principal location, and contact information (including email address) of data stewards should be readily accessible.

Commentary: The revised Openness Principle is nearly identical in substance to the 1980 version but is presented differently to provide greater clarity.

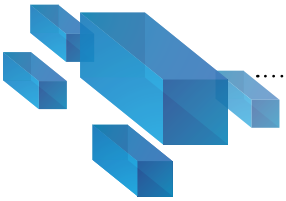
6. Security Safeguards Principle—Personal data should be protected by reasonable security safeguards against external and internal risks including unauthorised loss, access, destruction, use, modification, or disclosure.

Commentary: The Security Safeguards Principle is nearly identical in substance to the 1980 version but has been expanded slightly to clarify that the obligation to protect personal data extends to internal as well as external risks.

7. Accountability Principle
    a. Anyone who collects, uses, or otherwise processes personal data should be a responsible steward of the data and, to that end, should:
        i. be accountable for complying with measures that give effect to these Principles;
        ii. provide appropriate redress to individuals consistent with these Principles;
        iii. be liable for reasonably foreseeable harm caused by the data steward's failure to give full effect to these Principles;
        iv. upon reasonable request of a regulator, be able to demonstrate that the data steward has developed and implemented appropriate risk assessments, policies, processes, and procedures designed to follow data processing rules consistent with these Principles.
    b. No one should be held accountable under these Principles for any act or omission concerning data that is not personal data.

Commentary: The Accountability Principle in the 1980 Guidelines is both brief and vague: "A data controller should be accountable for complying with measures which give effect to the principles stated above." The revised principle is broader and more demanding. Under it, data stewards are not only responsible for compliance, but also for being able to demonstrate to regulators that they have in place the tools to comply. Moreover, under the new Accountability Principle, data stewards must provide injured individuals with redress and must accept liability for "reasonably foreseeable harm" caused by the failure to act accountably. These changes are all consistent with the shifting of responsibility for data protection from individuals to data stewards.

In addition, the new principle clarifies that accountability is focused on "personal data," which under the Definitions includes "any information that identifies an individual, could reasonably be used to identify an individual, or is linked to data identifying an individual and used in any manner affecting that individual." Accountability is not required for other data under these principles unless that data is (again referring to the Definitions) "linked to data identifying an individual and used in any manner affecting that individual" (although accountability may well be required by laws serving objectives other than data protection). This language gives the principles broad scope but precludes their application to data that is truly unconnected to individuals.



8. Enforcement Principle
    a. Nations should have in place adequate regulatory arrangements, competent bodies, and appropriate financial and human resources to ensure that laws enacted pursuant to these Principles are enforced.
    b. Enforcement of data protection laws should achieve effective compliance with these Principles and applicable law, while minimizing the burden on individuals and on lawful information flows.

Commentary: The 1980 Guidelines had no Enforcement Principle, but more than 30 years' experience has demonstrated the importance of ensuring that data protection laws are not merely adopted but also vigorously enforced. Under the new Enforcement Principle, governments are required to invest financial and human resources to enforce data protection laws and are reminded that, consistent with the 1980 Guidelines, the goal of enforcement is to "achieve effective compliance" while "minimizing the burden on individuals and on lawful information flows."

Appendix

GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA
Adopted by the Council of Ministers of the Organisation for Economic Co-operation and Development on 23 September 1980[15]

1. Collection Limitation Principle—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle—Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 [3] except:

   a) with the consent of the data subject; or

   b) by the authority of law.

5. Security Safeguards Principle—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

[14] The complete text of the 1980 OECD Guidelines and accompanying explanatory comments are available at www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

7. Individual Participation Principle—An individual should have the right:

   a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

   b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

   c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

   d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle—A data controller should be accountable for complying with measures which give effect to the principles stated above.