

HIPSSA Project

Support for Harmonization of the ICT Policies
in Sub-Sahara Africa,

TRAINING /DATA PROTECTION LAW
Zimbabwe, July 2013

Pria Chetty,
ITU International Expert on Data Protection



Summary of the Content

- Revisit and explain key concepts and definitions
- Examples and cases of principles of data protection law in practice
- Explanation of Transborder Flow restrictions in data protection law



WHY ENACT DATA PROTECTION LAW IN Zimbabwe?



With new promise comes new perils: ICTs and the right to privacy in Africa

BY: CARLY NYST ON: 30-NOV-2012

SHARE:   



One of the first things that strikes you about the chaotic East African metropolises of Kenya, Uganda and Zimbabwe is the blanket of adverts for mobile phone companies that covers them, from the walls of the immigration hall at Harare airport, to the rickety shacks that line the dusty streets of Kampala. Where official signage is unavailable, DIY versions are painted onto the roofs and walls of houses and small businesses. Stores selling mobile phones are rarely more than a few short steps away, as are the clumps of cell towers that stand tall above throngs of people talking, texting and transferring money on their mobile devices. The message is clear: mobile telephony has arrived in Africa, and everyone wants - and can have - a piece of it. But at what price?

A team from Privacy International has spent the past few weeks travelling in the region, hearing many stories of the significant advances achieved through the use of new technologies, particularly mobile ones. The most famous of these is undoubtedly Kenya's M-PESA mobile money system, which allows individuals to bypass traditional financial infrastructure and access and transfer money by SMS. In the first three months of M-PESA's operation, 111,000 people registered for the service, and nearly US \$6 million was transferred; today it is used by a quarter of the of the population, some of whom had not previously used mobile phones or owned bank accounts. Many people we spoke to told us of the importance of M-PESA to regular Kenyans, particularly those living in poverty, who for the first time have access to the financial system and the ability to save money and accumulate assets.

We also witnessed how communications technologies more generally are enabling greater connectivity, facilitating the flow of information, and engaging and empowering communities. We met with some amazing civil society groups that are using technologies to advance the effectiveness of their advocacy. The Human Rights Network for Journalists in Kampala uses podcasts and livecasts to get their message out, while the Zimbabwe-based Kubatana disseminates information through a SMS and email newsletter service. Organisations such as the Media Institute for Southern Africa, headquartered in Namibia, and the Kenyan Ethical and Legal Issues Network make savvy use of Twitter, Facebook, YouTube and email to reach their constituencies and make sure their voices are widely heard.

<https://www.privacyinternational.org/blog/with-new-promise-comes-new-perils-icts-and-the-right-to-privacy-in-africa>

"As the tide of technology sweeps across Africa, its manifestations - biometric databases, digitised border systems, electronic voting, communications surveillance, e-Health systems, mobile money - are being designed and implemented with little consideration for how such systems will protect the personal information of individuals and respect their private lives and decisions. Even more worryingly, these "advances" are being adopted without accompanying legal protections and safeguards to ensure that individuals' basic rights are protected. Such safeguards include data protection legislation..."



MARCH 13, 2013, 9:45 AM

Researchers Find 25 Countries Using Surveillance Software

By NICOLE PERLROTH

Last May, two security researchers volunteered to look at a few suspicious e-mails sent to some Bahraini activists. Almost one year later, the two have uncovered evidence that may be using off-the-shelf surveillance software to spy on their own citizens.

Morgan Marquis-Boire, a security researcher at Citizen Lab, at the University of Toronto's Munk School of Global Affairs, and Bill Marczak, a computer science doctor, discovered contained surveillance software that could grab images off computer screens, record Skype chats, turn on cameras and microphones and log keystrokes. The word was from a British company that says it sells monitoring software to governments solely for criminal investigations.

Now, one year later, Mr. Marquis-Boire and Mr. Marczak have found evidence that FinSpy is being run off servers in 25 countries, including Ethiopia and Serbia.

Until Mr. Marquis-Boire and Mr. Marczak stumbled upon FinSpy last May, security researchers had tried, unsuccessfully, for a year to track it down. FinSpy gained notoriety in 2012 when it was discovered a document that appeared to be a proposal by the Gamma Group to sell FinSpy to the government of President Hosni Mubarak.

Martin J. Muench, a Gamma Group managing director, has said his company does not disclose its customers but that Gamma Group sold its technology to governments to monitor pedophiles, terrorists, organized crime, kidnapping and human trafficking.

But evidence suggests the software is being sold to governments where the potential for abuse is high. "If you look at the list of countries that Gamma is selling to, including kidnappers and drug dealers, it looks more likely that it is being used for politically motivated surveillance."

As of last year, Mr. Marquis-Boire and Mr. Marczak, with other researchers at Rapid7, CrowdStrike and others, had found command-and-control servers running FinSpy.

The Munk School is publishing their updated findings on Wednesday. The list of countries with servers running FinSpy is now Australia, Bahrain, Bangladesh, Brazil, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, the United Arab Emirates, the United States and Viet Nam.

In Ethiopia, FinSpy was disguised in e-mails that were specifically aimed at political dissidents. The e-mails lured targets to click on pictures of members of Ginbot 20, which downloaded to their machines and their computers began communicating with a local server in Ethiopia.

"This continues the theme of FinSpy deployments with strong indications of politically motivated targeting," the researchers wrote in their report.

A Turkmenistan server running the software belonged to a range of I.P. addresses specifically assigned to the ministry of communications. Turkmenistan is the first clear-cut case of a government running the spyware on its own computer system. Human Rights Watch has called Turkmenistan one of the world's "most repressive countries" and warned that dissidents faced "constant threat of government reprisal."

In Vietnam, the researchers found evidence that FinSpy was running on Android-powered phones. They found one Android phone infected with FinSpy that was sending text messages back to a Vietnamese telephone number. That finding was

<http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/?pagewanted=print>

Human Rights Watch, at least 40 people had since been convicted and sentenced to prison terms. Many are now serving terms ranging from three to 13 years.




25 governments, many with questionable records on human rights, may be using off-the-shelf surveillance software to spy on their own citizens

E-mails contained surveillance software that could grab images off computer screens, record Skype chats, turn on cameras and microphones and log keystrokes

frequently used "against paedophiles, terrorists, organized crime, kidnapping and human trafficking

Privacy and policing databases: European Court ruling in M.M v. the United Kingdom

BY: CAROLYN MOELLER ON: 21-MAR-2013

SHARE:   



In November 2012 the European Court of Human Rights (ECtHR) ruled in *M.M.v. the United Kingdom* that retention and disclosure of a job applicant's police records to potential employers was incompatible with the European Convention on Human Rights. The Court ruled that the practice cannot be regarded as being in accordance with the law. This judgment is a key step in establishing privacy rights over data held by the police, and comes at an important time when governments are rewriting the rules around data retention and disclosure practices in the criminal sphere.

The case concerns M.M (the applicant) who abducted her grandson for three days in 2000 in order to prevent the girlfriend of her son from going back to Australia with the applicant's grandson. The UK Director of Public Prosecutions considered the case as a family issue and a minor offence. He therefore administered a caution, instead of pursuing court proceedings.

In 2003, in reply to a query from the applicant, the police advised that her caution would remain on records for five years. In 2006 M.M was rejected for a job dealing with childcare due to the disclosure of her criminal record.

In 2008 regulations were established to identify when and how information could be disclosed when offenders apply for jobs dealing with children and vulnerable adults. The purpose of the regulatory change in 2008 was to increase security of vulnerable individuals after the Soham murders. However, the new regulations led to the more frequent disclosure of data related to with very minor offences.

Subsequent to these changes, the Criminal Records Office informed M.M. that all convictions and cautions where the injured party is a child are kept on the record system for life.

When elaborating the permissibility of the retention and disclosure of M.M's caution data, the ECtHR evaluated first the admissibility of the complaint under Article 8. Interestingly, the Court declared the case admissible not because the applicant exhausted all domestic remedies (as is usually required) but because the UK Government did not afford reasonable prospects of success when challenging data retention. The Court came to this conclusion since data retention and data disclosure practices had never been successfully challenged in the UK.

Subsequently the Court analysed whether the violation of M.M's right to privacy was justified under Article 8(2). The Court concluded that the UK lacked a clear legislative framework for the collection and storage of data. There was no clarity as to the scope and restrictions of the powers of the police to retain and disclose caution data. Additionally, there were no mechanisms for

Case shows the reliance on personal information for decision making and negative impact

M.M abducted her grandson for 3 days to prevent son's girlfriend from leaving country with grandson

Minor offence and caution but on record for 5 years

M.M was rejected for a job dealing with children

Records kept for life

<https://www.privacyinternational.org/blog/privacy-and-policing-databases-in-the-uk>



Committed to connecting the world



CONCEPTS IN PERSONAL INFORMATION PROCESSING



Data Controller Retains Ultimate Responsibility despite other persons acting on its behalf

“data processor” refers to a natural person, legal person, or public body which processes personal information for and on behalf of the controller and under the data controller’s instruction, except for the persons who, under the direct authority of the controller, are authorised to process the data;

“data protection officer” or “DPO” refers to any individual appointed by the data controller charged with ensuring, in an independent manner, compliance with the obligations provided for in this law;

“data controller's representative” or “controller's representative”: refers to any natural person, legal person or public body permanently established on the territory [of the concerned country], who takes the place of the data controller in the accomplishment of the obligations set forth in this law;



Confused over whether you are a data controller or a data processor? Then read this

Published April 3, 2012 Contract Law , Data Protection , Outsourcing [Leave a Comment](#)

Under UK data protection laws, an organisation that processes personal data will be either a data controller or a data processor (a party that processes data on behalf of a data controller). The data controller is responsible under data protection laws for ensuring that data processed by it and its data processors is carried out in accordance with data protection laws. This will also include responsibility for any data security breaches by its data processors.

For this reason, it is important that you know what role your organisation plays in the processing of personal data.

Indeed, in commercial contracts, a supplier may seek a contractual statement that it is acting as a data processor of the customer. By doing this, the supplier will seek to contractualise the customer's responsibility for compliance with data protection laws (including, most crucially, the adequacy of the supplier's information security measures), and ensure that the supplier has no direct obligations under data protection legislation in relation to the processing that it undertakes under the contract.

However, sometimes it is not clear cut as to whether a party is acting as a data processor, or a data controller in its own right. Simply because you are doing something under a contract with another organisation does not mean that you are always going to be acting as a data processor.

New ICO guidance

To help organisations, the UK Information Commissioner has published a [new guide](#) to assist organisations with identifying their role.

As an example, the ICO's guidance states that lawyers, accountants and doctors will generally be data controllers in relation to the services that they provide, whereas a company providing outsourced services like payroll or mail marketing to another company is likely to be a data processor.

All change?

<http://techblog.brodies.com/2012/04/03/confused-over-whether-you-are-this/>

Who is controller and processor?

Organisations that process personal data –= data controller or data processor or representative.

Data controller – responsible for compliance including security breaches.

In Contracts – a statement that a supplier is acting as a data processor must be in place and confirmation of responsibility of data controller to customer

People remain unclear as to roles and how to determine

Lawyers, accountants and doctors are data controllers

Outsourced service providers are data processors acting on behalf of data controllers

data protection laws, reducing some of the benefits of "data processor" status.



Committed to connecting the world



European
Commission



Example 1

Credit reference agency data

A credit reference agency obtains, records, holds, organises, adapts, alters and discloses personal data. It is clearly a data controller for the data it processes. The agency customer/subscriber consults, obtains or retrieves personal data disclosed to it by the agency, but that is not sufficient for the data to be controlled jointly or in common. The customer/subscriber will process the data it has obtained, in a manner it alone determines, to inform a decision on whether to supply a customer, and is therefore a separate and distinct data controller. The customer does not have any authority over what the credit reference agency does with the data it holds.

Example 2

ContactPoint

The DCSF is building and maintaining a database of children, carers and key contacts. The creation of this database, its administration and its access to information are established in the Children's Act and supporting Regulations. The administration of this database is shared between DCSF and Local Authorities, e.g. DCSF manage database security and Local Authorities determine who may access to data, so between them they are joint data controllers for the data and have documented arrangements for satisfying data controller responsibilities. Other organisations that supply data to ContactPoint or who access data held within it are not data controllers as they do not determine the purpose or manner of processing within the ContactPoint database. They are data controllers in their own right for their own data as they determine, within the constraints of the Children's Act, how data, including the data obtained from ContactPoint, will be subsequently processed and for what purposes.

Agency obtains, records, holds, alters, discloses data

Customer consults, obtains, retrieves data

Agency – data controller

Customer – separate and distinct data controller

Data controller established in regulations

2 Public Bodies administer database of children, carers and contacts – joint data controllers

<http://www.apira.co.uk/userfiles/files/Data%20Controllers%20in%20common.pdf>



Committed to connecting the world





Information Commissioner's Office

Identifying 'data controllers' and 'data processors' Data Protection Act 1998

Contents

Overview	2
What the DPA says	2
Key consideration in determining who is a data controller - Degree of latitude/discretion/independence of the service provider	3
Different types of client and service providers	5

http://www.ico.gov.uk/for_organisations/guidance_index/~/_media/documents/library/Data_Protection/Detailed_specialist_guides/data_controllers_and_data_processors.ashx



Committed to connecting the world



Defining Personal Information

- *Identifiable Information*
- *Examples:*

Personal Descriptors

Name, age, place of birth, date of birth, gender, weight, height, eye color, hair color, fingerprint

Identification Numbers

Health IDs, Social Insurance Numbers (SIN), Social Security Numbers (SSN), PIN numbers, debit and credit card numbers

Ethnicity

Race, colour, national or ethnic origin

Health

Physical or mental disabilities, family or individual health history, health records, blood type, DNA code, prescriptions


Source: Privacysense.net



BUT in addition to information about you, personal information includes information about what you do, what you like, your preferences, behavioural data and your personal profile. Companies have a commercial interest in knowing you.

New "Irresponsible" Netflix Contest May Violate Customer Privacy

By David Coursey, PCWorld

Sep 22, 2009 9:57 AM | 

A privacy researcher is urging Netflix to cancel its next research contest, before it results in potentially millions of dollars in damages for invasion of its customers' privacy.

"Netflix should cancel this new, irresponsible contest," Paul Ohm wrote in a blog affiliated with Princeton University's Center for Information Technology Policy.



On Monday, the company awarded \$1 million to the winners of its first competition, aimed at developing technology to improve its ability to predict what movies its customers will like.

Ohm worries the information the company is about to release as test data for the second contest isn't as anonymous as Netflix may think.

According to the New York Times:

"The new contest is going to present the contestants with demographic and behavioral data, and they will be asked to model individuals' 'taste profiles,' the company said. The data set of more than 100 million entries will include information about renters' ages, gender, ZIP codes, genre ratings and previously chosen movies."

Ohm counters that "researchers have known for more than a decade that gender plus ZIP code plus birth date uniquely identifies a significant percentage of Americans (87% according to Latanya Sweeney's famous study.)"

"True, Netflix plans to release age not birth date, but simple arithmetic shows that for many people in the country, gender plus ZIP code plus age will narrow their private movie preferences down to at most a few hundred people."

Netflix – research contest

Awarded \$1 million – competition to develop technology to improve the ability to predict what movies customers will like

Test data for second competition is not sufficiently anonymous?

Demographic and behavioural data to model individual profiles. Data set of 100 million entries – ages, gender, ZIP codes, genre ratings and chosen movies

Gender, birth date, ZIP code – ID 87% of Americans

Gender, ZIP code and movie preferences – narrow to a few hundred people.

http://www.pcworld.com/article/172373/New_Irresponsible_Netflix_Contest_May_Violate_Customer_Privacy.html



Committed to connecting the world



European
Commission



Processing of Personal Information

The Act limits processing of personal information to place conditions on how personal information may be used.

- To prevent unintended uses of personal information
- To prevent abuse of personal information



Technology

THE BUSINESS AND CULTURE OF OUR DIGITAL LIVES,
FROM THE L.A. TIMES

Facebook digs through user data and graphs U.S. happiness

October 6, 2009 | 3:50 pm



Comments 0

+1 0

Tweet 0

Recommend 90

Facebook released a graphical breakdown showing the collective happiness of the site's millions of active U.S. users.

The company combed its database of short user-updates and looked for words indicating a theme of happiness or sadness correlating to the day it was posted. The breakdown was released Monday.

What we learned from the analysis of our nation's Web chatter: Holidays make people happy, celebrity deaths make people sad.

As Facebook notes, Thanksgiving and Christmas are some of the happiest days, while the deaths of **Heath Ledger** and **Michael Jackson** were among the lowest.

Indeed, the findings are completely obvious, but could become more interesting with years of data collection -- especially when aligned with economic indicators.

But, hey, do we really want Facebook to keep peering into updates meant just for friends and family? The research serves as a good reminder about cybersecurity -- after all, it is **National Cybersecurity Month**.

If you put something on Facebook, no matter how tight your privacy settings are, Facebook Inc. can still hang onto it, analyze it, remix it and repackage it.

Despite its silly name, the **Gross National Happiness** indicator is creepy. We're in there.

Mint, a personal finance website similar to (and now owned by) Quicken, also does this sort of data analysis. The company combs through millions of bank and credit card accounts that its users inputted for the purpose of *personal* finance tracking -- key word being "personal" -- in order to determine "**America's most frugal cities**" or "**global wealth distribution**."

<http://latimesblogs.latimes.com/technology/2009/10/facebook-happiness.html>



Facebook processing data for happiness index

What makes people happy?

Data aligned with economic indicators can be of interest

No matter how tight the privacy settings are, Facebook Inc. can use it, analyse it, remix it and repackage it.

Mint processes millions of bank and credit card accounts for personal finance tracking.

How comfortable are we with back-end processing?



International
Telecommunication
Union

Committed to connecting the world



What is sensitive?

(a) information or an opinion about an individual which reveals or contains the following

- (i) racial or ethnic origin;
 - (ii) political opinions;
 - (iii) membership of a political association;
 - (iv) religious beliefs or affiliations;
 - (v) philosophical beliefs;
 - (vi) membership of a professional or trade association;
 - (vii) membership of a trade union;
 - (viii) sex life;
 - (ix) criminal, educational, financial or employment record;
 - (x) gender, age, marital status or family status,
- (b) health information about an individual;
- (c) genetic information about an individual; or
- (d) information which may be considered as presenting a major risk to the rights of the data subject.

Often this information is used against the person when making a decision e.g. whether to employ or do business with a person

Information should not be used for purposes that the data subject has not consented to (with exceptions)

Privacy Commissioner Case Note

Case Citation:

W v Pathology Clinic [2008] PrivCmrA 24

Subject Heading:

Disclosure of sensitive personal information

Law:

National Privacy Principle 2.1 in Schedule 3 c

Facts:

The complainant had medical tests at a pathology clinic and asked that the results be provided only to their treating medical specialist and solicitor. The test results were to be part of a claim that the complainant was making to a federal government agency. The complainant later became aware that the clinic had provided the results directly to that government agency.

Australian Privacy Commissioner case

Information was disclosed for a purpose other than the primary purpose for which it was collected, and the disclosure was not permitted by any of the exceptions

The Commissioner formed the view that the disclosure was an interference with the complainant's privacy

Conciliation and Settlement

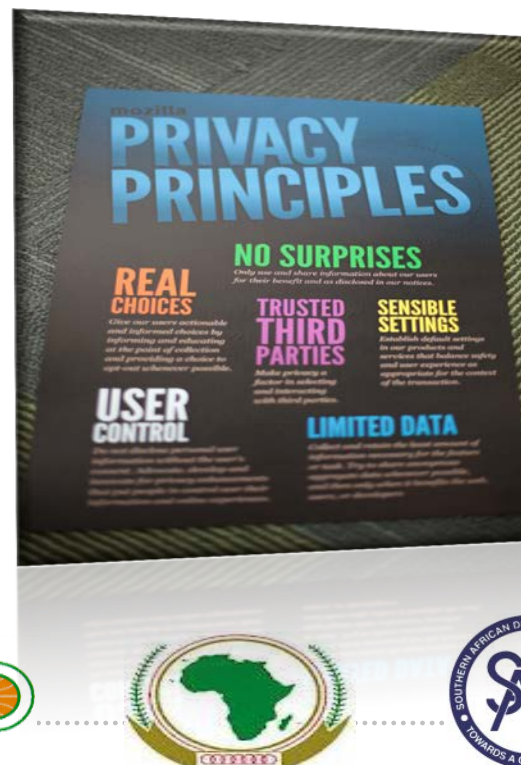
<http://www.privacy.gov.au/materials/types/casenotes/view/5977>



Committed to connecting the world



PROTECTION OF PERSONAL INFORMATION



International
Telecommunication
Union

Committed to connecting the world



PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. 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.

Data Quality Principle

8. 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.

Purpose Specification Principle

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

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

Security Safeguards Principle

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

Openness Principle

12. 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.

Individual Participation Principle

13. 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.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Original OECD
Principles
Source: OECD
www.oecd.org



Key Provision Principles of Data Protection Bill

- Processing of personal information (General Limitations)
- Minimality, Retention of records
- Collection directly from the data subject
- Purpose specification and further processing limitation
- Security measures on integrity of personal information
- Information processed by an data processor of the data controller
- Security measures regarding information processed by an data processor
- Notification of security compromises
- Quality of information
- Notification to the Commission and to the data subject
- Access to and challenges of personal information
- Correction of personal information
- Data controller to give effect to principles
- Prohibition on processing of sensitive personal information





"THAT WILL BE \$28.75,...NOW IF I CAN JUST GET YOUR POSTAL CODE, PHONE NUMBER AND A SMALL BLOOD SAMPLE,..."

Example:
You should
notify the
data subject
of the
*Purpose of
Collection of
information*

Image Source: Office of Privacy
Commissioner (OPC)





"AT LEAST WE CAN HAVE LUNCH WITHOUT THE BOSS LOOKING OVER OUR SHOULDERS!"

Has the employer notified the employees?

Are employees (also data subjects) aware of *Purpose of Collection*?

In



International
Telecommunication
Union

Committed to connecting the world





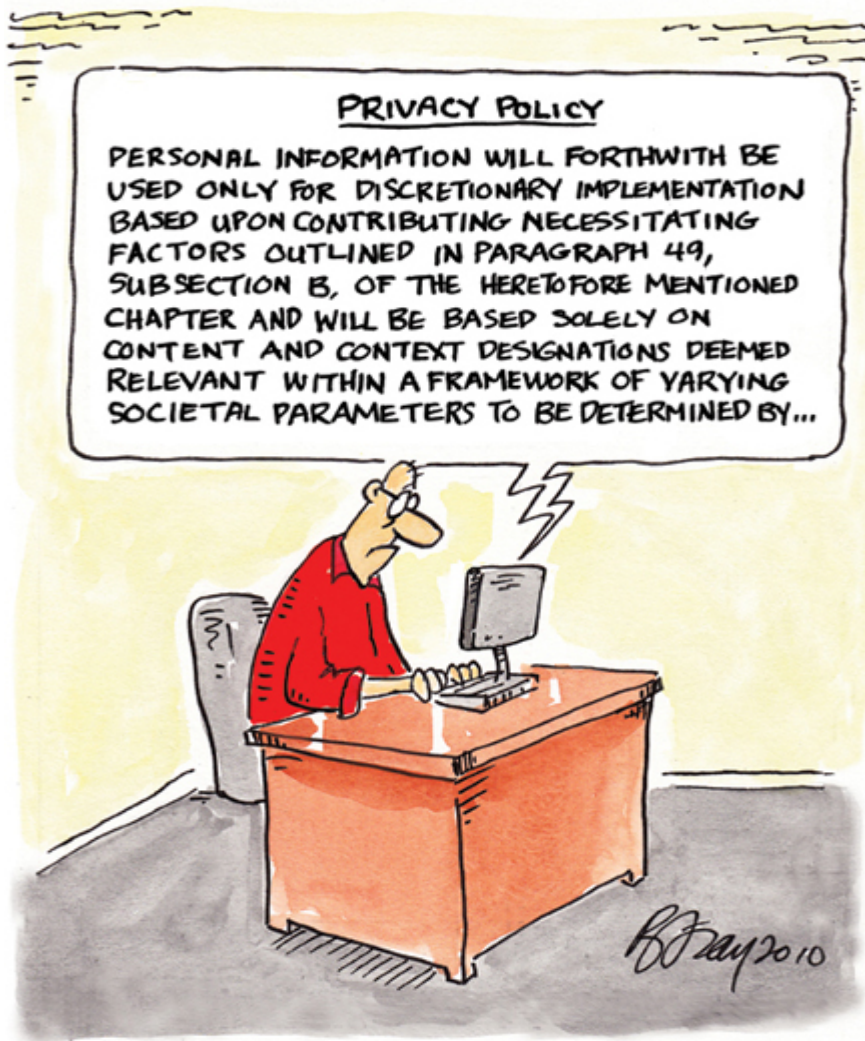
**Example:
Data
controllers
should have
necessary
security
safeguards
to protect
personal
information**

Image Source: Office of Privacy
Commissioner (OPC)



Principle: Security Safeguards

Image Source: Office of Privacy
Commissioner (OPC)



With the principle of notification, the data subject must understand the purpose of collection and how it will be used (not complicated legalese)

Image Source: Office of Privacy Commissioner (OPC)

Registration Number: Z5704402

Date Registered: 19 September 2001 Registration Expires: 18 September 2013

Data Controller: BRISTOL LAW SOCIETY

Address:

THE LAW LIBRARY
THE LAW COURTS
SMALL STREET
BRISTOL
BS1 1DA

This register entry describes, in very general terms, the personal data being processed

BRISTOL LAW SOCIETY

This register entry contains personal data held for 6 purpose(s)

Purpose 1

Staff Administration

Purpose Description:

Appointments or removals, pay, discipline, superannuation, work management or other

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Relatives, guardians and associates of the data subject

Data classes are:

Personal Details
Family, Lifestyle and Social Circumstances
Education and Training Details
Employment Details
Financial Details
Racial or Ethnic Origin
Religious or Other Beliefs Of A Similar Nature
Trade Union Membership
Physical or Mental Health or Condition

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

Data subjects themselves
Relatives, guardians or other persons associated with the data subject
Current, past or prospective employers of the data subject
Education, training establishments and examining bodies
Suppliers, providers of goods or services
Financial organisations and advisers
Central Government
Employment and recruitment agencies

Transfers:

None outside the European Economic Area

An example of notification by a controller to the Commission (Authority) of information collected and how it is processed.

= Principle of Transparency

Image Source: Office of UK Privacy Commissioner Website



International
Telecommunication
Union









Committed to connecting the world



UK says Google needs further privacy improvements

A review found that Google has improved privacy protections in its products but more work is needed

By Jeremy Kirk
Tue, August 16, 2011

  Share     Like 0   + Briefcase More

IDG News Service — Google was praised on Tuesday by the U.K.'s data protection watchdog for strengthening its privacy policies but the agency said the company still needs to improve.

Google has been under scrutiny by the Information Commissioner's Office (ICO) since the company admitted in May 2010 to collecting payload data from unencrypted Wi-Fi networks it was indexing as part of its Street View imagery program.

The ICO said in November 2010 that Google broke the law with the data collection, which in some cases recorded entire e-mails, passwords and URLs. The ICO declined to impose a fine and instead demanded that Google submit to an audit of its privacy policies.

The audit took place last month, the [ICO said in a statement](#). "The audit found that Google has taken action in all of the agreed improvement areas," the agency said. "The ICO has now asked the company to go further to enhance privacy, including ensuring that users are given more information about the privacy aspects of Google products."

Google is training its engineers now on advanced data protection and overall is paying more attention to privacy issues when products are designed, the ICO said.

But Google should also ensure that its products have a so-called "privacy story," used to educate users about products' privacy features. While Google has implemented a "privacy design document" for products, those documents should be checked for accuracy. Also, the core training for engineers should include specific design principles that come from the privacy design document, the ICO said.

Google's director of privacy for product and engineering, Alma Whitten, [wrote in a blog post](#) on Tuesday that the ICO's report "verifies the improvements we've made to our internal privacy structures, training programmes and internal reviews and identifies some scope for continued work."

"We know that there is no perfect solution, so we will continue to improve our current processes and develop new ones so that privacy awareness grows and evolves alongside Google," Whitten wrote.

Principles:
Transparency
Security
Safeguards

Source:
www.cio.com



Organisations and industries develop codes of conduct

Complaint Resolution Adjudicator

Obligations at least equal to principles

Members of public have an opportunity to comment

New private sector provisions in the Privacy Act 1988 (Cth) (the Privacy Act) regulate the way the private sector organisations collect, use, keep secure and disclose personal information. The private sector provisions aim to give people greater control over the way information about them is handled in the private sector by requiring organisations to comply with ten National Privacy Principles (NPPs).

The NPPs set the base line standards for privacy protection. However, organisations or industries may have and enforce their own privacy codes. The Privacy Commissioner (the Commissioner) must approve the code first, but once it has been approved the code will replace the NPPs for those organisations bound by the code. The Commissioner can revoke a code.

Options for complaint resolution

A code can include its own complaint handling mechanism. If it does, it must provide for the appointment of a complaint adjudicator to handle complaints. A code adjudicator would be bound by the processes spelled out in a code when handling complaints and must meet the requirements of the Privacy Act and the Code Development Guidelines.

A code that incorporates a complaints handling mechanism can give industry a sense of ownership in developing a dispute resolution system operating in an organisation/industry that is equipped to handle complaints.

If a code does not provide for a complaint handling mechanism, the Office of the Privacy Commissioner will be the code adjudicator.

Code approval

Before a code can be approved, the Privacy Act requires the Commissioner to be satisfied that:

- the obligations in the code are, overall, at least the equivalent of the NPPs; and
- the members of the public have been given an adequate opportunity to comment on a draft of the code.

If the code includes a complaints handling mechanism, the Commissioner must also be satisfied that the code:

- provides for a code adjudicator; and
- meets the prescribed standards and the Commissioner's guidelines in relation to making and dealing with complaints.

Organisations not bound by a code must comply with the NPPs set out in Schedule 3 of the Privacy Act, in these circumstances. A copy of the NPPs is available on the Commissioner's web site or by contacting the Commissioner.

Considering the resource requirements

Organisations will need to be aware that developing and implementing a privacy code will necessarily require resources. The costs will vary greatly from scheme to scheme with likely variants being whether or not the scheme is a stand-alone code, the size and nature of the organisation/industry that will be covered by the code, and the nature of the code.

There are also several steps involved in developing a code that will require an allocation of resources. These steps include: identifying the need for a code, writing and publishing the code, seeking external legal or professional advice, implementing the code, and training staff. There could also be costs involved in:

EXAMPLE OF CODES OF CONDUCT BEING DEVELOPED BY INDUSTRIES,

IN ZIMBABWE INDUSTRIES CAN DEVELOP CODES ON HOW PERSONAL INFORMATION WILL BE TREATED



Implementation

Policies

- Privacy Policy (internal)
- Privacy Policy (external)
- Information Security Policy
- Monitoring Policy
- Records Management Policy

Contracts

- Consent
- Third Parties
- Data Processors
- Data Controller's Representative
- Employees/ Contractors

Assessments

- Technical
- Compliance Assessments

Privacy

We highly value your trust in choosing Booking.com for your online accommodation reservation. Therefore, we will duly and diligently safeguard and protect the privacy and confidentiality of your personal details, including your credit card details. This privacy policy applies to all of our services, whether accessed or made available online or through any other platform or device (hereafter collectively referred to as the "Website"). By accepting this privacy policy you consent to the processing of your personal data by Booking.com for the purposes specified below.

Why we process your personal data

Booking.com processes your personal data for the following purposes:

- 1) Making reservations via the Website.
- 2) Evaluating your stay at a location booked through the Website, and placing this evaluation on the Website.
- 3) Informing you about interesting offers (only with your consent).

We may also use your personal data to detect fraud and/or other illegal acts aimed at Booking.com.

Personal data collected by Booking.com

Booking.com collects the following personal data: your name, address, email address, telephone number, payment details, booking history, reservation preferences and smoking preference. This information is required to process, book and manage your reservation.

Booking.com may also process data about your computing device such as IP address, browser type, and operating system (or mobile device) Unique Device Identifier, operating system, application version and latitude/longitude. This information is collected to improve our services, but may nevertheless be considered personal data either by themselves or when combined with other information. This information is processed in accordance with European data protection law.

Transfer to third parties

Under certain conditions Booking.com may transfer your personal data to the following third parties:

The accommodation you booked

For the purpose of completing your booking we will disclose your name, contact details and the credit card details to the relevant accommodation with which a booking is made. We will only provide those elements to the accommodation that are required for it to process your reservation.

By completing a booking, you agree to be invited to complete our guest review form. If you wish, the review can be completed anonymously. By completing the guest review, you agree that it can be used on our Website on the relevant accommodation information page and on other such platforms and social media (wholly or partly) owned, controlled, managed or hosted by us or our trusted business partners for the sole purpose of informing future customers on the service level and quality of the relevant accommodation. We reserve the right to adjust, refuse or remove review forms at our sole discretion. The guest review form should be regarded as a survey and does not include any commercial offers, invitations or incentives whatsoever.

Data processors

From time to time, we may use third party service providers as data processors for the purposes specified above. For example, we may use service providers to send reservation information to accommodations electronically. Processing by these third parties takes place under our instruction. These parties are bound by data processing agreements and confidentiality agreements.



International
Telecommunication
Union

Committed to connecting the world



Example of Privacy
Policy of
Booking.com
www.booking.com
Last update: July
2012

TRANSBORDER FLOW OF PERSONAL INFORMATION



Transborder Flow

- "transborder data flow" term that arose in the 1980s following concerns in the EU regarding the value of information and the exchange of information across countries
- between business units of one company, data processing services or purposes ancillary to the commercial engagement.
- Includes transfer of human resources, financial records customer information: marketing and travel, and for public sector agencies (law enforcement, border controls and tax agencies).
- In Zimbabwean Bill, restrictions are placed on personal information sent outside Zimbabwe

Reference: **TRANSBORDER DATA FLOW: EU DIRECTIVE AND IMPLICATIONS FOR INTERNATIONAL BUSINESS**
Elizabeth Longworth, New Zealand



Application

- An adequate level of assurance is needed as to how information will be treated
- Countries - adequate level of protection – determined by assessment of e.g. the laws and policies of country
- Where country does not have adequate laws:
 - Data Subject Consent
 - Transfer is necessary (for specific legitimate reasons)
 - Other Authorisation
- Contracts can be used to place obligations on foreign recipient
- Article 26(2) of the EU Directive: *Three conditions in order to guarantee a minimum level of protection: the purpose limitation principle, restrictions on onward transfers and the data importers' undertaking of providing the data subjects with the rights of access, rectification, deletion and objection*

Reference: **TRANSBORDER DATA FLOW: EU DIRECTIVE AND IMPLICATIONS FOR INTERNATIONAL BUSINESS**
Elizabeth Longworth, New Zealand



Guidance on the use of cloud computing

Cloud computing is an example of transborder flow of personal information as information is hosted at a foreign destination

Consult Guide Issued by the UK Information Commissioner

<http://www.ico.gov.uk/>



Example

An organisation wishes to expand its online presence to include social media. The organisation develops a third party application to run within a social network platform.

The organisation will be a data controller for any personal data it processes through users choosing to use its application, integrated with the social network or for any other data collected through usage of the application.

The social network platform will be acting as a data controller for any personal data processed by the social network. This may also include processing done for advertising or marketing purposes.

Where the personal data is being used by both organisations for their own purposes, they will both be data controllers.

N.B. With transborder flow, data protection responsibilities still reside with the data controller.

Source: Guidance on the use of Cloud Computing, issued by the UK Information Commissioner

<http://www.ico.gov.uk/>



Committed to connecting the world



In closing: TRENDS/ CHALLENGES



Worldwide, approximately 1.1 million identities were exposed per breach, mainly owing to the large number of identities breached through hacking attacks. More than 232.4 million identities were exposed overall during 2011. Deliberate breaches mainly targeted customer-related information, primarily because it can be used for fraud.

[Internet Security Threat Report Volume 17](#),
Symantec, April 2012

Drone Surveillance

Re-identification

Facial Recognition

Behavioural Advertising

Location Data

Thank You

Questions?

Pria Chetty

International Legal Expert on Data Protection

(e) pria.chetty@gmail.com

(t) +27 (0) 83 384 4543



Image Credits

- Slide 22

photo credit: <http://www.flickr.com/photos/lhirlimann/6161838643/> Ludovic Hirlimann via <http://photopin.com> <http://creativecommons.org/licenses/by-sa/2.0/> cc

