Protecting Digital Personal Information from the End User Point of View

Abstract

Personal Information, both Private and Work information, is today very often managed in digital form and at risk of loss or unauthorized distribution. Most of this Information is created and managed directly from the End User who is often not in the condition to manage its security. In this article we describe what this information is and discuss what can be done to improve its security.

The loss of Personal Information is on the front pages of most newspapers almost every day. With "loss" of Personal Information it is usually intended some information related to a person that is made public without the authorization or against the will of its owner.

There are many ways in which this can happen, and we restrict ourselves to cases where the Personal Information is stored in digital form and managed by digital devices, from the smallest smart-phones and similar gadgets like digital watches etc., to the largest company servers.

What can a typical user do to better protect her digital Personal Information?

And what can be done by the IT community to protect the digital Personal Information of the users?

In this article we make an overview of the problems and some approaches that are currently considered even if, it is important to state it immediately, no real completely satisfactory solution seems to be available.

The whereabouts of Digital Personal Information

We need to start by understanding what is Personal Information in this context. We can define it as any kind of information related to the person that has limited or null distribution. In other words, it is any kind of information regarding or related to the person to which the person herself or someone else owning the information, attaches some constraints on who should be able to access it and how.

In technical, IT terms, we would define digital Personal Information some information of which the user-person is the owner or manager and to which is attached an Access Control List (ACL) limiting the access to it to any user-person. In an extreme case, the access can be limited also to herself: for example the user-person can declare the information to be read-only to everybody, herself included, to prevent any modification ever.

There are two main classes of this Personal Information:

- Private Information: this is information related to the private, eg. not work related, life of the person: this information can be related to her family, her friends, her beliefs etc.; this information can be related only to the person herself, like in the case of beliefs, or be linked to other persons, like in the case of family, friends etc.
- Work Information: this is information related to the work aspects of the person's life; typically this information is related also to other persons' work and some information can actually be owned and governed by someone else, as in the case of Company information created and managed by the person; with a few exceptions, this information is shared with someone else but has a limited or at least controlled distribution.

The main difference between Private and Work Information is that for Private Information the person is totally in control of it, whereas for Work Information usually the ownership and control are shared or even completely under the control of others. Obviously in the two cases the kind of information and the relation with the other people involved are different. Still the overall problem is the same: controlling information that is created and/or managed by the person and that must have limited distribution and access.

Examples of such Personal Information can be the following:

- the person's bank account credentials
- the person's credit card data
- the person's best friends' names, telephone numbers, addresses
- the person's religious and political beliefs etc.
- the company's new product specifications
- the company's access codes to the manufacturing buildings

- etc.

This information can be directly valuable, as bank account credentials or credit card data, or indirectly valuable such as information about the person or the company the person works for, that can damage or benefit the public image of the person or company.

Distinguishing Private and Work Information

Is it possible to distinguish between Private and Work Information?

In theory we can, but in practice it is much more difficult. For example some of our work colleagues are also friends and it is normal for companies to help employees to have relations also outside the office. Moreover, in many companies, for more efficiency, we can work from home and we can bring to work our own devices (BYOD).

This means that we bring in our private life part of our working life and vice-versa. Being so, it becomes very difficult to clearly and neatly classify and divide information according to the Private versus Work criteria. As a practical example it is much easier to have a mailbox for John which contains all kinds of correspondence with him, from the next barbecue with the families to the most restricted company documents.

If companies impose very strict rules in managing company information, they limit the efficiency of the employees, in some circumstances making it more difficult or even impossible to access information. This protects the information but it can imply that some work is delayed or not done at all.

From the person's point of view, the managing of information should be straightforward and intuitive, classification should be easy and fast both to store the information and to retrieve it, like in the case of the John's mailbox above.

So in practice we are not very good at dividing Private and Work Information, unless the company we work for has implemented very good Security Policies about Work Information.

This makes it much more difficult to protect the Information since most of the time we do not know which kind of protection should be applied to it. The military approach, in IT starting from 1970s, requires to apply a Label, that is a classification, to each piece of information produced and managed. As of today, this approach is practically impossible for Personal Information, we are just not able to manually label each piece of data we create and manage on our IT devices: documents (files), pictures, emails, movies etc.

We end up protecting the Information by compartment or, more often, by device.

This bring us to the following situation: In practice all information managed and stored on a single device is considered to have the same security classification and is protected in the same way, even if in reality the device manages and stores information of many different types, values and security significance.

The storing and managing whereabouts of Information

Another important issue to consider is where, that is in which devices, the information is managed and stored. In general we can identify two classes of devices:

- the End User devices, like PC, portable computers, tablets, smart-phones but also smart-watches, televisions and soon refrigerators and other IoT devices managed by the user;
- the Service Provider devices, that is any device which provides services to the users but it is not owned or under the control of the user: as of today these are typically services delivered through internet by remote servers as for example all the "Cloud" services; these include also the company's servers and other devices which are directly managed by a company and connected directly to the company network.

The last point requires a clarification: some companies provide their employees with devices like portable computers, tablets or smart-phones which are directly managed by the company itself and directly and exclusively connected to the company network. Even if physically not present at the company's premises, these devices are logically internal to the company. The user cannot manage them and can access internet or IT services outside the company only passing through the company IT systems. They are thus equivalent to any IT devices physically internal to the company.

For simplicity we assign these devices to the Service Provider devices' class, even if the user can manage on them also Private information, as she can do when she is physically at the company's premises.

In principle the End User devices managed only by the company and logically internal to the company's IT systems should constitute another class of devices, in between the previous two. But for our present purposes this difference can be ignored.

For the rest of this article we will consider the issue of protecting Personal Information on End User devices.

Protecting the End User devices

As already mentioned, we cannot expect a typical end-user to apply different protection policies to each type of information. So the starting and quite often only protection measures should be applied at the device level and to all information managed and stored by it.

In the last years the following security measures have become de facto standards for protecting the End User devices:

- periodic security updates in some cases performed in the background and totally without user intervention;
- use of a security suite of programs like: personal firewall, anti-virus, anti-malware, anti-phishing etc.;
- disk and full device encryption;
- anti-theft applications and procedures for portable devices.

These security measures are the basis for any security of the End User devices. To help the users, these measures should be applied automatically and independently of the user. This is possible, even if not yet applied to all devices like smart-phones and smaller devices, for updates and security suite of programs when installed and configured appropriately, step which can require the intervention of the user at least initially.

The device encryption is a very important security measure but it is subtle and often used incorrectly, giving a false sense of security to the user. First of all, it requires to manage a password or a token from which is derived the cryptographic key which is used to encrypt and decrypt the data. This often requires the User to choose and memorize a good secret password or manage another security token. Moreover, once the device is running, the data is accessed in clear (decrypted on the fly) by the device and by whoever has access to it. Only when the device is completely turned off, at rest, then all data is encrypted and not accessible. Instead the typical user never turns off the device, which hibernates but still does not delete the decryption keys (notice that de device does not ask for the key/password when it is woken up). In this case, encrypting the data on the device has very limited effects.

The anti-theft applications, which include also the simple addition of a password to the BIOS and boot-loader of a PC, are becoming more common, in particular with smart-phones and services that offer to locate the devices when they are stolen. Again they often require the user to create and manage other secret passwords.

So the security of the End User device still relies mostly on the End User herself. There are quite a few in principle easy things that the End User could do to improve the security of the information managed by her IT devices on top of the ones just mentioned. Some of these measures are:

- encrypt all backups, UBS keys, external disk and devices;
- do not manage really very sensitive information on IT devices at all;
- do not share sensitive information between different devices whenever possible;
- use a Password Manager, even better a local Password Manager and not a Cloud Password Manager service; this allows the user to create and manage strong and individual passwords for each service, backup drive or backup service, web applications etc. which requires them with the exception of the passwords for the BIOS, the boot-loader, the disk/device encryption, the local account and the Password Manager itself (still these are quite a few passwords);
- never use the same password for two different services or purposes, for example if a zip encrypted file (see below) is shared with other users, use a different password for each user and better still, change all passwords every time a new version of the file is shared;
- organize very sensitive information in groups and encrypt them individually on disk (on top of the full disk encryption); this can be done with dedicated file or file-system encryption programs but also more easily, even if not with the same features and security level, with encrypted zip archives, managing the passwords of each archive with the Password Manager (and remembering to close the archive when it is not any more used);
- share sensitive information with other devices, in the “Cloud” etc., only if encrypted, for example in encrypted zip archives as mentioned above.

There are also other, a little more advanced measures for example to protect the privacy of the user like using private / incognito browsing or Tor and Tor browsing, or using special operating system designed for security and privacy like Tails, Liberte, Privatix, IprediaOS and other live OS. But obviously this is just the tip of the iceberg of the security measures, processes and procedures that can be applied.

Unfortunately most of the measures and procedures presented are still too complex for the typical user of an IT device. Slowly some form of awareness and education on the secure use of IT devices is arriving to all the End Users, but we cannot expect that all End Users will be able to master even half of the security measures that have just been presented.

This leaves us with only one possibility: to provide the End User the needed security without the need of active cooperation by the End User herself.

For what concerns Work Information, this is possible and should not be a too difficult target to reach. Indeed Work Information are owned and/or managed by companies which should have the personnel, expertise and tools to implement security policies, including user awareness, to manage securely the information.

The more difficult problem is how to help the End User to protect her Private Information. In this case the IT service providers, including hardware and software providers, should work hard to invent and provide more out-of-the-book security services to the End User that require the minimum intervention by the End User herself.

We will discuss in a future article these issues in more detail.

Andrea Pasquinucci (PhD CISA CISSP)