26TH INTERNATIONAL CONFERENCE ON PRIVACY AND PERSONAL DATA PROTECTION
WROCLAW, 14 SEPTEMBER 2004

Amendment to 2003 Conference Resolution on Automatic Software Updates

Resolution

Following a proposal by the Office of the Australian Federal Privacy Commissioner, the Information and Privacy Commissioner of Ontario, Privacy Commissioner for Personal Data for Hong Kong and Commissioner for Data Protection and Access to Information for the State of Brandenburg the International Conference resolves that:

1. The Conference notes with concern that software manufacturers worldwide increasingly use non-transparent techniques to transfer software updates to users' computers. In doing so they:
   - can read and collect personal information stored on the user's computer (e.g. browser settings, and information on the user's browsing habits) without the user being able to notice, to influence or to prevent it,
   - may gain at least partial control over the target computer thereby restricting the ability of the user to meet his legal obligations and responsibilities as a controller to ensure the security of any personal data he may be processing,
   - change the software installed on the computer which will then be used without any required testing or clearance and
   - may bring about malfunctions in the updated computer without the possibility to identify the update as the cause.

   This may cause particular problems in government institutions and private companies to the extent that they are under specific legal obligations how to process personal information.

2. The Conference therefore calls on software companies:
   a. to offer procedures to update software online only with notice and execute the update after obtaining consent of the user, without exceeding or abusing their consent, in a transparent way and without allowing unchecked access to the user's computer;
   b. to ask for the disclosure of personal data only with the informed consent of the user and insofar as it is necessary to carry out the online update. Users should not be forced to identify (as opposed to authenticate) themselves before they can initiate the download process;
   c. to provide for update services which allow for prior testing on detached servers before installation.

3. The conference encourages the development and implementation of techniques to update software which respect the privacy and autonomy of computer users.

Explanatory Notes

The purpose of this paper is to provide some background information about the proposed amendments to the resolution adopted by Commissioners at the 2003 Conference on automatic software updates. The resolution was sponsored by Alexander Dix and was based on work by the International Working Group on Data Protection in Telecommunications. The resolution is listed as Resolution No 4 on the Resolutions page of the 2003 Conference website:
www.privacyconference2003.org/commissioners.asp

The 2003 resolution expressed concern with non-transparent techniques to transfer software updates to user's computers, which had the potential to allow software manufacturer's partial control and access to information stored on the user's computer.

Since the resolution was published, Microsoft has been in contact with a number of Commissioners, including Alexander Dix, Ann Cavoukian, her deputy Ken Anderson and former Australian Federal Privacy Commissioner Malcolm Crompton. Microsoft has made a convincing case that parts of the resolution as adopted in the 2003 Conference are either impossible to implement or counter productive. By counter productive, it is meant that implementation of the resolution could actually delay some updates even when they are urgently necessary.

The need for very rapid updates stems from the fact that most viruses and hacker attacks occur after a software update has been released. Hackers and virus writers often find software vulnerabilities through reverse engineering software updates to find what they are fixing. In such circumstances, it is extremely important to get a software update (sometimes called a patch) out to as many people as possible in the shortest period possible. This prevents hackers and virus writers from taking advantage of the lag time between public release of the update and its widespread adoption, to devise viruses and attack software weaknesses. Literally every hour of delay could increase the scale of the damage caused worldwide.

Inhibiting the fast adoption of software updates could harm privacy by giving hackers a window of opportunity in which to access personal information on individual's computers.

Linked to this Microsoft has made a number of comments about the 2003 resolution, which relate to how the resolution could be counterproductive.

Microsoft stated that:

> "Since distributing patches quickly is critical to protect the health of the Internet as well as the privacy of its users, CD-ROM distribution cannot be the method of choice (i.e., the portion of the resolution which discourages online updates is very problematic). First of all, CD-ROM distribution cannot be accomplished with sufficient speed, especially if worms are being released within hours of a bulletin. Second, a CD is burned at a point in time and may not be current when finally installed by the user (e.g., a patch may have been modified or additional patches may have been issued). Although there is certainly a value in releasing CDs (especially for very large patches or to bring a non-compliant system up to date by providing a number of service packs and/or patches), only online upgrades can ensure that users have an opportunity to install the most recent patches before a worm strikes their system or a hacker gains unauthorized access to steal PII.
>
> It is also not clear to us why patches be provided only at the user's request or initiative, as opposed to providing notice and choice to the end user. We know, of course, that some automobile users will not take the initiative to "buckle up" even though failure to wear a seat belt subjects one to death or severe physical injury (not to

> mention, in some jurisdictions, penalties imposed by police forces!). In light of this reality, a process requiring notice and choice would seem to strike a better balance between privacy through patching and user control.
>
> Finally, we propose replacing the text related to "unchecked access," mostly because it is unclear what this phrase means. The OS itself has unchecked access to the system; it makes little sense to suggest an upgrade (especially to the kernel of the OS) cannot have unchecked access as well. Moreover, if the vulnerability being patched provides root access to the system, then the software vendor, a criminal, and anyone else with technical knowledge and skill has "unchecked access"; that is why patching is so critical"[1].

In response, to Microsoft's comments Alexander Dix has worked closely with the Microsoft people on a proposal to amend the resolution. The aim was to preserve the initial privacy protection of the resolution, but to make it workable. As a result, Alexander Dix drafted an amended resolution.

The amended resolution was emailed to Commissioners on the 12 April 2004, with a letter from Australian Federal Privacy Commissioner Malcolm Crompton detailing the reasons that it was felt that the amendment was necessary. However, only eight replies were received. It was then decided that it was necessary to bring the resolution back to the conference to secure a stronger consensus.

The proposed change will amend the 2003 Conference Resolution from:

1. The Conference therefore calls on software companies
    a. to offer procedures to update software online only at the user's initiative or request, in a transparent way and without allowing unchecked access to the user's computer;
    b. to ask for the disclosure of personal data only with the informed consent of the user and insofar as it is necessary to carry out the online update. Users should not be forced to identify (as opposed to authenticate) themselves before they can initiate the download process;
    c. To provide for freedom of choice by offering online updates only as an alternative to other (offline) means of software distribution such as CD-ROM.

To:

2. The Conference therefore calls on software companies
    a. to offer procedures to update software online only with notice and execute the update after obtaining consent of the user, without exceeding or abusing their consent, in a transparent way and without allowing unchecked access to the user's computer;
    b. (unchanged)
    c. to provide for update services which allow for prior testing on detached servers before installation.

As the convenor of the 2003 conference the Office of the Federal Privacy Commissioner of Australia is proposing this resolution with the sponsorship of the Commissioners of Brandenburg, Ontario and Hong Kong. The changes as distributed in April 2004 have the support of the Commissioners of Ireland, Spain, the German Federal Commissioner, the Netherlands and the EU Data Protection Commissioner.

---

[1] Excerpts from a letter sent by Scott Charney from Microsoft to Ann Cavoukian. On 12 April 2004 the letter was circulated by e-mail to Commissioners who attended the resolutions section of the 2003 Data Protection and Privacy Commissioner's Conference by the incumbent Australian Federal Privacy Commissioner Malcolm Crompton.

If Commissioners agree to the changes to the resolution, we will see strong industry support for implementing the modified resolution, led by Microsoft. This would be an outstanding example of 'practical privacy', with Commissioners having significantly impacted on real world business practices.