

Big Brother Doesn't Keep Your Assets Safe

Dr. Johannes Wiele
LANline

Motivation

- Employee monitoring tools sold as IT security solutions
- Statistics misused for marketing by fear
- Lobbyists try to weaken employee privacy rules
- PR departments and agencies work hard to influence journalists by sending out annoying amounts of horror stories about employees misusing corporate IT infrastructure

Quotes to keep in mind

- „Seventy-eight percent of organisations identify risk reduction as their top influencer for information security spending“
(Ernst & Young Global Information Security Survey 2003)
- „The behaviour of employees is a source of uncertainty and unpredictability in any organisation’s environment“
(Surveillance & Society 1 (2) 2003, p. 152-190, www.surveillance-and-society.org)
- „People often make security trade-offs for non-security reasons [...] – Don’t blindly accept that `It’s for security purposes` when someone tries to justify a questionable coutermeasure“
(Bruce Schneier in „Beyond Fear“ [2003, p.279])

Part one

Who says **what** to **whom** to **achieve**
what under **what** **circumstances**?

(Basic journalist's question)

What is said?

- „You lose money because your employees surf the web and chat with their friends by e-mail“
- „They send out confidential content“
- „They store dangerous content in your network“
- „Increased employee monitoring is necessary to increase information security within an organisation“
- „Employee privacy can be dangerous“

What is said?

- Employee monitoring is less expensive and more effective than authentication, authorisation, document security and identity management
- „Install a technical surveillance solution and get the employees‘ consent to monitoring, and everything will work out fine“

Who says it?

- Consultants
- Lawyers
- Vendors of monitoring solutions through their marketing and PR teams
- Politicians
- Employers' organisations
- Managers

To whom?

- CEOs
- CSOs
- Board members
- Politicians
- The public through journalists

Under what circumstances?

- Businesses are forced to reduce risks
- Economic crisis
- The employees' negotiating position is weakened
- Resulting from acts of terrorism surveillance gets a brighter image

„Risk reduction as a top influencer for information security spending“

- Legislation and financial regulation require risk management (Basel II, Sarbanes Oxley...)
- Risk management is often reduced to risk reduction
- Taking risks has gained a bad reputation
- Employee surveillance seems to be a suitable measure to reduce business risks
- Technical solutions can be presented more easily than organisational measures like communications practises and employee training

Statistics fuel fears

- Most questionnaires ask for fears, not for real incidents – because no one will talk about information security breaches that happened to her or his company
- Therefore the results automatically strengthen the fears
- Most managers can easily imagine disgruntled employees taking revenge for unpopular measures, but they don't expect to be a target of industrial espionage
- By many statistics only misjudgements are confirmed
- The „insider threat“ is misunderstood ...

Statistics fuel fears

- The 80:20 rule about the internal threat is questionable – mistakes are counted in the same way as acts of criminal intent
- The internal threat gets more important because the solutions against external threats are working more and more successfully. Employees don't misbehave more often.
- Do you know you all of your „insiders“?

...To achieve what?

- To increase security
- and / or -
- To sell strategies, services and legal advice
- To sell monitoring tools, filters and forensic software (the „Internal threat“ was discovered when firewall selling slowed down)
- To pave the way for the acceptance of surveillance



GEGEN HACKER, VIREN UND WÜRMER SIND SIE GESCHÜTZT.
ABER WAS IST MIT ROSEMARIE AUS DER PERSONALABTEILUNG?

eTrust™ Security-Lösungen
Umfassende Sicherheit für Ihr gesamtes Unternehmen.

Manchmal lauern Gefahren da, wo man sie gar nicht erwartet. Gut, wenn man eine Sicherheitslösung hat, die das Unternehmen vor allen möglichen Angriffen schützt, ganz gleich, ob sie von außen oder von innen kommen. eTrust ist die Antwort auf diese Sicherheitsfragen. Unsere Produktfamilie schützt nicht nur Ihr gesamtes Unternehmen, sie bietet Ihnen darüber hinaus die Möglichkeit, Ihre Sicherheitsinfrastruktur zu überwachen und zu managen, sei es zentral oder von verschiedenen Standorten aus. So können Sie Ihr Unternehmen weiter ausbauen und Ihre Chancen maximieren, während Sie gleichzeitig Ihr Risiko minimieren. Das nennen wir Sicherheit, auf die Sie vertrauen können.

Portraying Employees as
criminals:

Marketing by Fear

Easy to combine with
„dumb user“ resentments
of administrators against
end users.

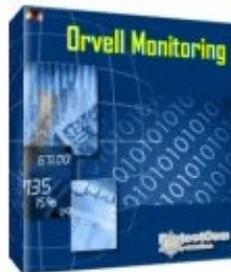
Tools get more invasive

- Keylogging is actively propagated
- Proactive forensic tools interrelate business software use with phone call, web usage and e-mail
- Results are stored for a longer time
- Corporate surveillance invades the private life of homeworkers
- Monitoring „Work in Progress“ is a special problem – an employee should be able to decide for himself when her or his work is ready to be presented to others

Tools get more invasive

Visuelle PC Überwachung - für Büro und Zuhause

Neu: Orvell Monitoring: visuelle PC Überwachung



Orvell Monitoring 2005 - nimmt in regelmäßigen Abständen den Bildschirminhalt auf und speichert die Daten versteckt auf der Festplatte. Orvell ist zur vollständigen visuellen Überwachung aller Computeraktivitäten entworfen - **ausführlich bis zum letzten Tastenanschlag.**

Neue Version: grafische Analyse und Auswertung der PC Nutzung, eMail Alarm bei Anschluss von USB Sticks, Profi Tastaturrekorder (Keylogger) und vieles mehr. € 59.95 - **deutsche Version.**

Weitere Informationen über [Orvell Monitoring 2005](#)

Spector Pro: der Überwachungsklassiker



Spector Pro 5.0 - jetzt mit einem eMail Rekorder zur Aufnahme von verschickten und empfangenen eMails von GMX, Yahoo.de, Hotmail und dem deutschen AOL!

Spector Pro ist eine der leistungsfähigsten und intelligentesten Softwarelösungen zur PC Überwachung, die weltweit erhältlich ist: eMail-/Chat-/IRC Rekorder, Keylogger, Bildschirmaufnahme und sogar einem Peer to Peer Rekorder zur Aufzeichnung von Tauschbörsen! € 99.95 - **englische Version.**

Weitere Informationen über [Spector Pro 5.0](#)

PC Überwachung mit eMail Versand - für Büro und Zuhause

Part two

**Why employee monitoring does not fit
into IT security strategies:**

The drawbacks of monitoring

Resistance

- Monitoring is understood as a sign of mistrust
- In Europe employees expect a certain level of privacy at their workplace (and they can)
- Consent does not break resistance
- The request for consent may be understood as a compulsory measure
- Resistance to monitoring results in indifference towards other security measures – „If they don't trust me, let them do their stuff alone“

Resistance

- There's often no discussion about or information flow on security measures
- Sometimes even policies are missing
- In Physical Security, avoiding resistance to security measures is a key element to create safety.

„Never tell the attendees of an event where they are not allowed to go – tell them where to find coffee and free lunch“.

Some Remarks on „Trust“

- Trust is an economic idea – it reduces costs by making it unnecessary to constantly monitor those who work for you
- To profit from trust always implies taking the risk of being deceived
- Surveillance means to abandon trust – there is no workaround
- Statistics show that information sharing only works in an atmosphere of trust

Benefits from Trust

Less well-known statistics:

„Freedom at Workplace“ sometimes makes people work harder...

Romanticism?



Benefits from Trust

2002 National Technology Readiness Survey (NTRS) co-sponsored by the Center for e-Service at the University of Maryland's Robert H. Smith School of Business and Rockbridge Associates, Inc., a market research firm in Great Falls, VA.



Summary to be found at <http://old-www.rhsmith.umd.edu/ntrs2002/>

Benefits from Trust

Home Internet Usage for Work Purposes Compared to Work Internet Usage for Personal Uses

(Source: 2002 National Technology Readiness Survey (Dec. 2002))

	Hours/week on Net while at home for work-related purposes	Hours/week on Net while at work for personal reasons
Base: Employees with online access at home/both home and work (<i>Mean</i>)	(125) 5,9 hours	(122) 3,7 hours
Base: Employees with online access at home only (<i>Mean</i>)	(35)* 3,7 hours	NA
Base: Employees with online access at work only (<i>Mean</i>)	NA	(27)* 6,5 hours
Base: All Adults with access at home or work	(160) 5,3 hours	(149) 4,4 hours

Note: responses do not include people who were unable to estimate the hours.

*Caution: small sample size

Benefits from Trust

- For many employees work does not end at 5 o'clock
- Surveillance and mistrust may delay the reduction of bureaucrazy in work organisation

Benefits from Trust

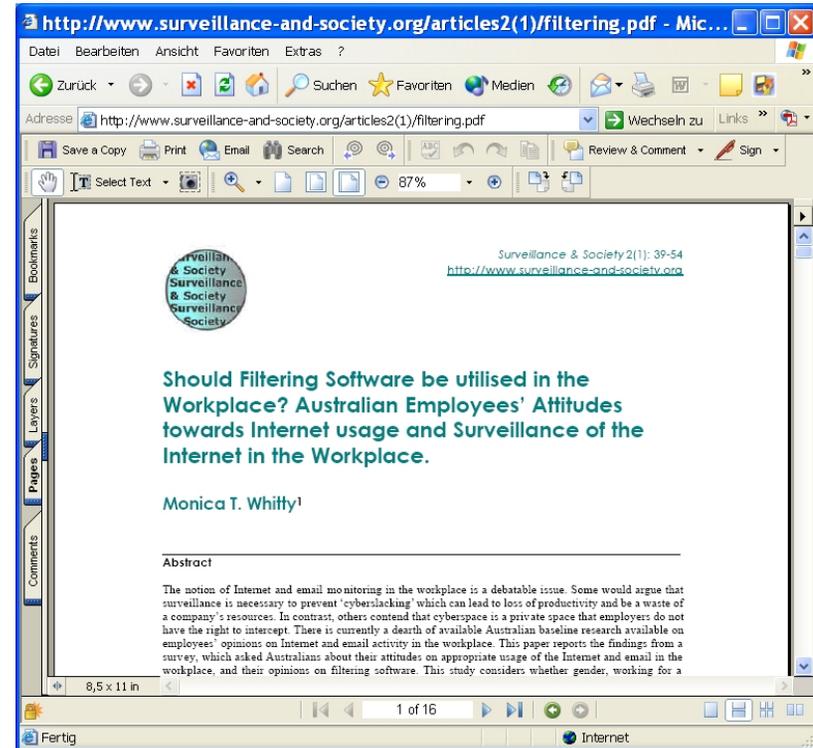
„Surveillance & Society“

Scientific researches on all aspects of surveillance in society and at the workplace

„Should Filtering Software be utilised in the Workplace?“

Australian Employees' Attitudes towards Internet usage and surveillance of the Internet in the Workplace“

(Monica T. Whitty)



To be found at <http://www.surveillance-and-society.org>

Benefits from Trusts

Conclusions from the Australian Study:

- „Although this study does contribute to this important debate, more research on the attitudes of Internet filtering in the workplace and how the Internet and email is used in the workplace is critical“.
- „The way forward is not to reduce the debate to outcomes of productivity. Instead [...] we need to take account of the worker’s opinions.“
- „[...] adopting an either/or view on Internet surveillance can be problematic.“
- „[...] future research might consider different types of workplaces as well as different levels of responsibility and level of management.“

Mistrust: Danger of Polarisation

tomorrow

E-MAIL UND SURFEN IM BÜRO

So werden Sie überwacht



SpionageCheck//03 Start | Ende | Checkliste: [Progress Bar] Spionagetour: [Arrow]

Zugriff des Administrators

//Outlookdaten
 //E-Mails
 //private Dateien
 //Passwortqualität

Hat Ihr Chef Ihnen schon einmal zur neuen Freundin gratuliert ??

automatische Datenspeicherung

//Cookies
 //Caches
 //Verlauf

Der Systemadministrator kann alle Adressen, Termine und Aufgaben, die Sie in Ihrem Terminkalender und Organizer (z.B. Outlook) gespeichert haben, einsehen. Er hat sogar die Möglichkeit, diese zu verändern, ohne dass sie es merken. Selbst wenn Sie die Termine oder Notizen als "privat" markieren, versperrt das dem Administrator den Einblick nicht unbedingt.

Weitere Überwachung

ver di

„Privates“ Surfen am Arbeitsplatz gibt es nicht: Egal, wie vorsichtig Sie sind – wenn Ihr Chef mitlesen will, kann er das auch. Wir zeigen, wo die Spionage-Tools schon überall herumschnüffeln, und wie Sie Ärger mit Ihrem Chef vermeiden können.

Foto: Photodisc

SatireWire | Survey Claims Work Doesn't Interrupt Personal Web Surfing - Microsof...

Datei Bearbeiten Ansicht Favoriten Extras ?

Adresse http://www.satirewire.com/news/0010/webwork_survey.shtml Wechseln zu Links >>

Economy of Errors The new book from **SatireWire** On Sale Now! [click here to learn more](#)

SatireWire

MARKET-LEADING PROVIDER OF NEW ECONOMY SATIRE SOLUTIONS

STUDY CLAIMS WORK NOT AN IMPEDIMENT TO PERSONAL WEB SURFING AT WORK
 Meanwhile, Policies Prohibiting Work During the Surfday Found Unproductive

SAN JOSE, CAL. (SatireWire.com) — More than 80 percent of respondents to a new LGI/Gallup poll admit they do "some" or "a lot" of work while at work, but almost all insist they never let business-related matters interfere with personal Web surfing at the office.

"When I come in at 8:30, I'm pretty much focused on surfing the Web for personal reasons," says survey respondent Barth Biggs, an account representative at Harmony Photo Imaging in Glenville, Ohio. "Occasionally, yeah, I'll switch over and do some business-related thing, but it's just a breather, and I mostly do it during lunch."

According to the survey, an overwhelming 86 percent of respondents say doing some work during the surfing day has no negative impact on their personal Web surfing. In fact, 48 percent say doing occasional work at work actually improves the quality of their personal surfing, and 28 percent also say it makes them happier and less stressed.



if employees are allowed to work at work, they become more productive personal Web surfers,

Economy of Errors CLICK HERE
 THE NEW BOOK FROM **SATIREWIRE**
 Ads by Goooooogle

Realtime Opinion Polls
 Post a Question & View Votes Live
 Massive Worldwide Audience
www.whatthenationthink

Presidential Decks
 2004 presidential election Kerry or Bush souvenir playing card decks
www.presidentialdecks.com

Home
Book
Archives
Features
Briefs
Charts
Popular
Reaction
Links
SW Store
About

Please Note
CAMEO
 Cool Estate Jewelry. Impress her for once.
FARK.COM
 It's not news, it's

Statistics
 —
 don't miss
 this one
 ☺

Side Effects of Anomaly Detection

- A fully automated employee monitoring relies on anomaly detection
- But: Not only fraud, also creativity results in anomalies and deviation
- To avoid attracting an anomaly scanner, it's best to do business as usual as quiet as possible and to strive for a conformist appearance and behaviour
- So surveillance may result in a loss of creativity
- By the way: Anomaly detection still does not work without being monitored itself

Monitoring means being too late

- Surveillance solutions often don't prevent information security breaches, they only make lawsuits easier
- Customers only honour preventative security
- **Prevention** is required by law!
- Monitoring may bring a company into conflict with privacy laws

Part three

Alternatives

Identity Management

- Single-sign-on solutions get ready for use
- PKI has successfully moved into applications
- Authentication, authorisation and identity management are integrated into management solutions

Document security

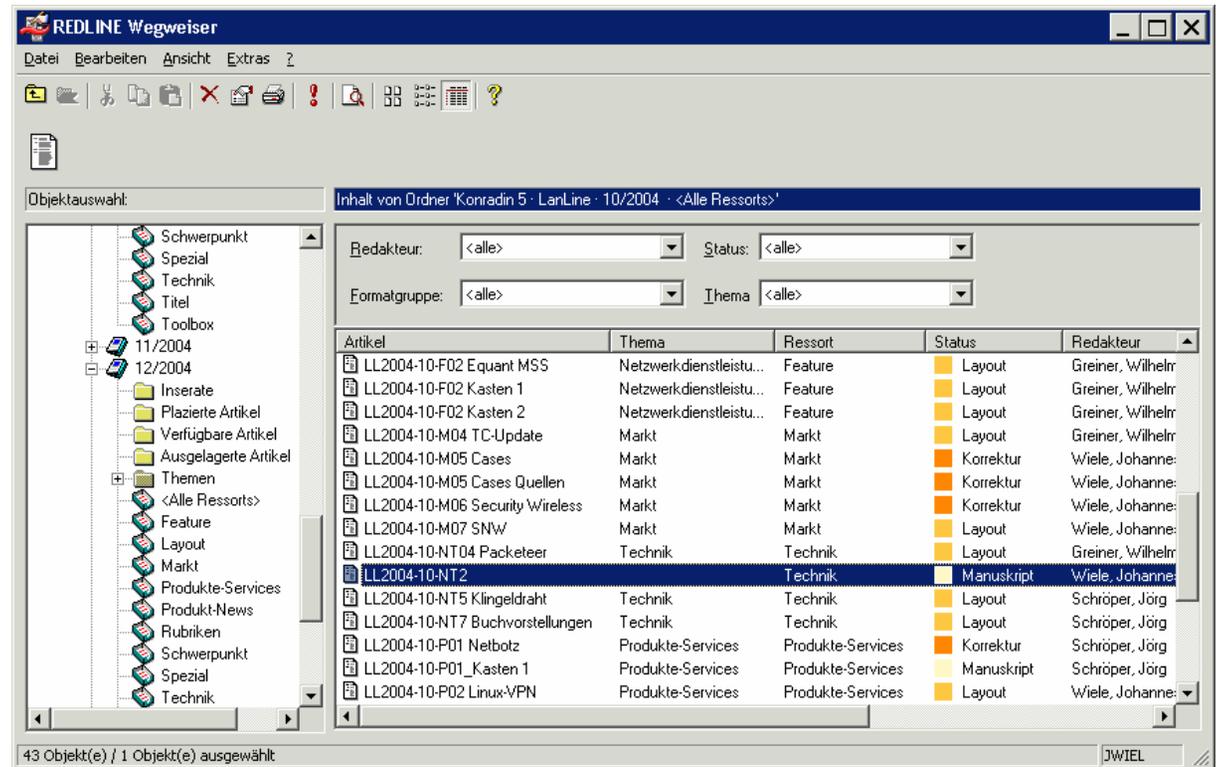
- With document security, practises known from the pre-computer era can easily be re-established
- Document security solutions prevent confidential documents from being misused

Network Partitioning

- Resources can only be accessed by those who really need access
- Security does not act as a show stopper in areas where unhindered communication is more important than security

Integration of Privacy Concepts with Security Concepts

- Provide personal free zones where surveillance is not allowed



Build a Security Communication Structure and Practises

- Don't leave security measures to technicians only – people are more trustworthy than appliances
- Discuss security measures with the employees to rise awareness
- Ask them what has to be secured – they know it best
- Be friendly – someone who is not sure if she or he has made a security-relevant mistake must be able to talk about it without fear

Conclusions

- Security should not act as a show stopper in areas where unhindered communication is more important than security
- Don't mix up security with other interests!

Contact

Dr. Johannes Wiele
www.lanline.de

wj@lanline.awi.de
johannes@wiele.com