

Security and Privacy Through the Lens of Norwegian Law

Kjell Jørgen Hole
NoWires Research Group
Department of informatics
University of Bergen

Last updated October 27, 2009

Overview—Norwegian acts and regulations

- Act on Financial Contracts and Financial Assignments
(“[Finansavtaleloven](#)”)
- Regulations on the use of information and communication technology
(“[IKT-forskriften](#)”)
- Personal Data Act (“[Personopplysningsloven](#)”)
- Personal Data Regulations (“[Personopplysningsforskriften](#)”)
- Discussion—why is it the security so bad despite acts and regulations?

Act on Financial Contracts and Financial Assignments

3

Financial Contracts Act—FCA

- Act on Financial Contracts and Financial Assignments ([Financial Contracts Act—FCA](#))
- In Norwegian: "Lov om finansavtaler og finansoppdrag av 25. juni 1999 nr 46" or "[finansavtaleloven](#)"
- Sections 34 and 36 are central to us

4

FCA Section 34.

Others' misuse of an account etc.

- (1) The account holder is not liable for others' wrongful withdrawal or other debit unless the person who effected the transaction identified him/herself in accordance with the rules of the account contract, and the debit was possible as a result of intent or **gross negligence** on the part of the account holder or someone entitled under the account contract to debit the account.

- **Consequences**

- An account holder in, e.g., an online bank is, in general, not responsible for losses caused by attacks from crackers or malicious insiders
- A banking solution should be designed in such a way that it is clear when the account holder is grossly negligent

5

FCA Section 36.

Modification of account holder's liability

- (1) Liability pursuant to sections 34 and 35 may be modified if the method by which the account can be operated is not satisfactory, or if the payment or account card system fails to meet sound standards as regards identification, control and warning routines, and the wrongful debit or the misuse is related to this. Account may also be taken of any lack of due care or other circumstances on the part of the institution that have been instrumental in enabling the wrongful debit or the misuse to take place.
- **Consequence.** **An online bank utilizing weak security mechanisms, e.g. weak authentication of account holders, may have to accept an extended responsibility for the account holders' assets**

6

ICT Regulations

7

ICT Regulations

- Regulations on the use of information and communication technology (ICT)
- In Norwegian: "Forskrift av 21. mai 2003 nr 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT)" or "[IKT-forskriften](#)"
- From the Financial Supervisory Authority of Norway (www.kredittilsynet.no)
- Sections 3 and 5 are of particular interest to us

8

ICT Regulations Section 3. *Risk Analysis*

- The institution shall establish criteria for acceptable risk with regard to use of its ICT systems
- The institution shall have a documented process for conducting risk analyses of its ICT activity. This process shall define responsibilities and shall include monitoring of steps taken as a result of the analysis performed
- The institution shall at least annually, or in the event of modifications of significance to ICT security, conduct risk analyses to ensure that risk is contained within acceptable limits in relation to the institution's business. The results of the risk analysis shall be documented

9

Consequences

- Risk analysis should be carried out during the development of new banking applications
- Important to develop good [architecture](#) and [design](#) documents to facilitate risk analysis
- Documents should be understandable both to developers and (external) security experts
- **Question to think about:** Should the risk analysis be made available to a customer (and his lawyer) during a conflict?

10

ICT Regulations Section 5. *Security* (not complete):

- Compliance with the requirements as to security in relation to personal data under Regulations No 1265 of 15 December 2000 to the Personal Data Act, shall be regarded as compliance with the provisions of this section.
- **Consequence.** It is important to verify that the security in an online banking system fulfill the requirements of the Personal Data Act

11

Personal Data Act

12

Personal Data Act

- Act relating to the processing of personal data ([Personal Data Act—PDA](#))
- In Norwegian: "Lov om behandling av personopplysninger av 14. april 2000 nr 31" or "[personopplysningsloven](#)"
- Section 2 defines **personal data** any "information and assessments that may be linked to a natural person"

13

PDA Section 13. *Information Security*

- Section 13 in the Personal Data Act considers information security aspects:
 - the controller of personal data shall by means of planned, systematic measures ensure the [confidentiality](#), [integrity](#) and [availability](#) of the data
 - the controller must document the data system and internal control measures
 - the documentation must be available to the Norwegian Data Inspectorate and the Privacy Appeals Board
- The act only sketches a framework for information security, detailed rules are found in the associated regulations

14

Personal Data Regulations

15

Personal Data Regulations—PDR

- Regulations on the processing of personal data ([Personal Data Regulations—PDR](#))
- In Norwegian: "Forskrift om behandling av personopplysninger av 15. desember 2000 nr 1265 ([personopplysningsforskriften](#))"
- Chapter 2, especially Sections 2-11 to 2-14, are central to us
- See also "Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer", Norwegian Data Inspectorate

16

PDR Section 2-11.

Protection of Confidentiality:

- Measures shall be taken to prevent unauthorized access to personal data where confidentiality is necessary
- **Consequence.** Techniques for identification, authentication, and authorization must be used to protect "sensitive" personal data
- The security measures shall also prevent unauthorized access to other data of significance for data security

17

PDR Section 2-11.

Protection of Confidentiality (cont.):

- Personal data that are transferred electronically by means of a transfer medium that is beyond the physical control of the data controller shall be encrypted or protected in another way when confidentiality is necessary
- **Consequence.** A client-server application transferring personal data over a public network (e.g. Internet) **must apply end-to-end encryption**
- **Remark.** WAP 1.x with WTLS cannot be used because the gateway has access to data in cleartext

18

PDR Section 2-12. *Securing of Accessibility:*

- Measures shall be taken to secure access to personal data where accessibility is necessary
- **Consequence.** Personal data must be protected by access control and/or encryption
- The security measures shall also secure access to other data of significance for data security
- Preparations shall be made for alternative processing in the event of the information system being unavailable for normal use
- Personal data and other data that are necessary to restore normal use shall be copied

19

PDR Section 2-13. *Protection of Integrity:*

- Measures shall be taken to prevent unauthorized changes in personal data where integrity is necessary
- **Consequence.** The integrity of personal data must be protected when stored in databases or files
- The security measures shall also prevent unauthorized changes in other data of significance for data security
- Measures shall be taken to prevent malicious software
- **Consequence.** OS and/or program environment must protect data against malicious software

20

PDR Section 2-14. *Security Measures:*

- Security measures shall prevent unauthorized use of the information system and make it possible to detect attempts to make such use
- Attempts to make unauthorized use of the information system shall be registered
- Security measures shall include measures that cannot be influenced or circumvented by members of the staff, and shall not be limited to actions that any individual member is supposed to carry out
- **Consequence.** Tamper-proof logs are needed
- Security measures shall be documented

21

If we have adequate laws, why are there still serious security and privacy problems?

22

Possible reasons (1)

- Major stakeholders believe that “each day nothing bad happens makes it less likely that something bad will happen in the future”
 - perfect setup for a “black swan”
- Many technical experts are not able to explain the need for security and privacy in a way that is useful to upper level management
 - understandable metrics are needed to quantify risks
- Since management does not fully grasp the need for security and privacy in information systems, they do not invest adequately in these areas

23

Possible reasons (2)

- There is little pressure on system owners to improve the security and privacy because the users often take the risk
- Since, as a general rule, Norwegian industry is not willing to discuss security problems openly, the industry as a whole is not learning from past mistakes
- “Security by secrecy” leads to strong emotional reactions when independent experts point out security weaknesses
 - little energy is used to fix the actual problem
 - more energy is used to attack the experts

24

Possible remedies

- **Openness:** System owners should be required to disclose information about the security and privacy of their systems during conflicts
- **Penalties:** Tougher penalties for system owners providing inadequate security and privacy to their customers
- **Education:** Better security education, e.g., at universities. All software architects and developers should have basic understanding of security and privacy issues
 - security experts must learn how to better explain security and privacy issues to management

25

References

26

- **Personal Data Act**

- English version: www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf
- Norwegian version: www.lovdatab.no/all/h1-20000414-031.html

- **Personal Data Regulations**

- English version: www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/POF_eng_v2.pdf
- Norwegian version: lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001215-1265.html

27

- **Personal Data Regulations (cont.)**

- Security comments in Norwegian: www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/SV100_00.pdf

- **Financial Contracts Act (“Finansavtaleloven”)**

- www.lovdatab.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/n1-19990625-046.html&emne=finansavtalelov*&

- **Regulations on the use of information and communication technology (“IKT-forskriften”)**

- www.lovdatab.no/cgi-wift/ldles?doc=/sf/sf/sf-20030521-0630.html&epslanguage=no

28

- M. J. Ranum, “The Anatomy of Security Disasters,” SOURCE Boston, March 11–13, 2009; www.ranum.com/security/computer_security/editorials/disasters/v2.pdf