Handboek Ethiek

Versie 1.2

Datum
20 juni 2016
Versie
Versie 1.1 –vastgesteld 11 februari 2014
Actualisatie vastgesteld 20 juni 2016

Inleiding 3

Statuut 4

Definities 4

Artikelen 4

Procedure voor het indienen van een onderzoekvoorstel 6

Procedure voor het uitvoeren van een onderzoeksproject 8

Juridische aspecten 8

Procedure voor het publiceren van een onderzoek 9

Responsible Disclosure

Onderzoeksfase

Communicatiefase:

Eindfase

Appendix I 11

Appendix II 11

Appendix III 16

Voorbeeld eerste communicatie 16

Plan van aanpak bij het vinden van een kwetsbaarheid 16

Inleiding

Tot voor kort waren ethische discussies alleen gericht op onderzoek waar mensen direct als onderzoeksobject bij betrokken zijn, zoals in het domein van de geneeskunde en de gedragswetenschappen. Door de steeds groter wordende overlap tussen het onderzoeksgebied van sommige meer exacte wetenschappen, zoals Information Science (IS), en het privédomein van mensen, is de ethische discussie echter ook hier belangrijk geworden. Dit wordt mede door de toename van interdisciplinair onderzoek steeds evidenter.

Zo wordt bijvoorbeeld door gedragswetenschappers de sociale media op het internet gebruikt voor gedragswetenschappelijk onderzoek, vaak met discussies over de privacy van data als gevolg. Deze nieuwe vorm van onderzoek roept dus tientallen nieuwe vragen op, zoals bijvoorbeeld…

1. Hoe wordt de autonomie van de deelnemers bewaakt?
2. Hoe weten we of een deelnemer de doelen van het onderzoek begrepen heeft?
3. Bij gebruik van sociale media: hebben deelnemer en onderzoeker dezelfde perceptie van privaat/publiek?
4. Hoe worden onderzoekdata beveiligd?
5. Door wie en hoe zijn de data doorzoekbaar?

Aan de andere kant staan de informatici, die onderzoek doen naar o.a. de beveiliging van netwerken en de toegang daartoe, waarbij ze vaak de zwakheden van een informatie systeem vinden. Vragen die hier van belang zijn, zijn onder andere….

1. Is de eigenaar van het IS op de hoogte van het onderzoek?
2. Welke methoden (ethisch of niet) worden er gebruikt om toegang te verkrijgen?
3. Hoe moet er worden omgegaan met een ontdekte zwakheid?
4. Hoe gaat men om met disclosures?

Deze voorbeelden illustreren de problematiek.

Om de integriteit van het onderzoek en de onderzoeker te waarborgen is het dan ook noodzakelijk om dat aspect in beschouwing te nemen. De onderzoekers moet een kader worden aangeboden waarbinnen zij hun doen en denken kunnen toetsen. Wanneer het onderzoek binnen die kaders valt, kan de onderzoeker rekenen op ondersteuning van het Instituut en neemt het Instituut voor Informatica de verantwoordelijkheid op zich.

Om de wetenschappelijke kwaliteit en de maatschappelijke relevantie van het onderzoek dat door het Instituut voor Informatica wordt verricht te garanderen, moeten onder andere de juridische en ethische aspecten van het onderzoek worden getoetst, zowel voor, tijdens en na het onderzoek. Hierbij wordt onderscheid gemaakt tussen standaard en niet-. De toetsing wordt uitgevoerd door Ethische Commissie Information Sciences (ECIS) van het Instituut voor Informatica van de Universiteit van Amsterdam.

In de navolgende hoofdstukken is veelvuldig gebruik gemaakt van het stuk 'PROCEDURE VOOR ETHISCHE TOETSING VAN ONDERZOEK AAN DE AFDELING PSYCHOLOGIE VAN DE UNIVERSITEIT VAN AMSTERDAM', November 2005, Commissie Ethiek, Afdeling Psychologie, Universiteit van Amsterdam .

Statuut

Definities

1. Standaard onderzoek binnen het Instituut voor Informatica:

In appendix I staat voor elke sectie beschreven welk onderzoek er plaatsvindt en onder welke randvoorwaarden. Een nieuw onderzoeksproject valt echter alleen onder deze definitie van Standaard onderzoek van het Instituut voor Informatica indien een onderzoek volledig kan worden geclassificeerd als 'standaard onderzoek' met behulp van de onderstaande beschrijvingen. Daarbij moet worden voldaan aan alle randvoorwaarden die bij het betreffende type onderzoek vermeld zijn en moet het onderzoek worden uitgevoerd door een onderzoeker van de betreffende sectie. In dat geval is het indienen van het onderzoeksvoorstel bij de secretaris van het ECIS voldoende.

2. Niet Standaard onderzoek binnen het Instituut voor Informatica

Alles wat niet valt onder Standaard onderzoek.

3. Theoretisch onderzoek binnen het Instituut voor Informatica

Onderzoek waarbij geen interacties met derden zijn.

4. Controversiële aspecten

Al die aspecten waarover (grote) juridische of ethische verschillen van mening bestaan.

5. ECIS

Ethische Commissie Information Sciences

Artikelen

1. Indien een onderzoek niet-standaard onderdelen en/of controversiële aspecten (zie definities) bevat en wordt uitgevoerd onder verantwoordelijkheid van het Instituut voor Informatica, dient dit te worden voorgelegd aan de Ethische Commissie Information Sciences (ECIS) voordat met de uitvoering wordt begonnen. Dat geldt voor onderzoek van stafleden, zowel als van AIO's, postdocs en studenten. Onderzoek dat geheel of gedeeltelijk wordt uitgevoerd binnen de verantwoordelijkheid van het Instituut voor Informatica dient altijd goedgekeurd te zijn door het ECIS. Een onderzoeker met een aanstelling of toelating bij het Instituut voor Informatica is altijd primair verantwoordelijk voor het onderzoek. Indien het onderzoek wordt uitgevoerd door een student, stagiair of ingehuurde kracht dient iemand van het Instituut voor Informatica daarvoor de verantwoordelijkheid te dragen. Ook onderzoek dat uit naam van iemand van het Instituut voor Informatica elders wordt uitgevoerd (bijvoorbeeld op een school, bedrijf of instelling) dient goedgekeurd te worden.

2. De ECIS heeft regels opgesteld met betrekking tot het uitvoeren van onderzoek en stelt op basis daarvan adviezen op over de toelaatbaarheid van onderzoek. Onderzoek dat niet van te voren is aangemeld bij de ECIS valt niet onder de verantwoordelijkheid van het Instituut voor Informatica, en wordt dus uitgevoerd op eigen risico, cq op persoonlijke titel. Naar aanleiding van maatschappelijke ontwikkelingen of ervaringen in het onderzoeksveld, kunnen regels veranderen en de toelaatbaarheid van onderzoek kan daardoor op elk moment ter discussie komen te staan. In alle gevallen heeft de ECIS het laatste woord over de

toelaatbaarheid van onderzoek en kan de ECIS ook reeds lopend onderzoek (uiteraard in uitzonderlijke gevallen) onderbreken. Deze regels zijn openlijk beschikbaar op www.ecis.ivi.uva.nl.

3. De ECIS streeft ernaar om de toetsingsprocedure zoveel mogelijk gestroomlijnd te laten verlopen, zodat de voortgang van het onderzoek zo min mogelijk wordt gehinderd. Extra administratieve belasting van de onderzoekers wordt zo veel mogelijk vermeden. Indien nieuw onderzoek volledig voldoet aan de eisen het geldt een verkorte procedure voor het voorleggen van het onderzoek aan de ECIS. De directeur kan toestemming geven om een onderzoek voorlopig te laten starten, maar het definitieve startsein kan in het geval van de normale procedure alleen worden gegeven door de ECIS als geheel.

4 .De ECIS bestaat uit een viertal stafleden* met brede ervaring en kennis. Zij worden benoemd voor een periode van een jaar. Deze leden hebben één of meerdere secties in hun portefeuille, maar niet de sectie waar ze zelf deel van uitmaken. De directeur van het Instituut voor Informatica is de voorzitter en wordt bijgestaan door een secretaris (het eerste aanspreekpunt) en (een) ter zake deskundig jurist(en) met kennis van informatierecht en bestuursrecht. De ECIS vergadert 6 maal per jaar en indien nodig op ad hoc basis om de voortgang van het onderzoek zo min mogelijk te belemmeren. Naar behoefte wordt het beleid van de ECIS bijgesteld en worden specifieke onderzoeksprojecten besproken die aan de ECIS zijn voorgelegd.

5. Onderzoek dat aan de ECIS als geheel wordt voorgelegd (en dus geen verkorte procedure ondergaat), wordt bij de eerstvolgende reguliere vergadering behandeld, of eerder indien daarvoor dringende redenen zijn. Een beslissing over goed- of afkeuring van onderzoek wordt dus altijd binnen twee maanden genomen, tenzij om nadere informatie gevraagd wordt. Indien die informatie niet tijdig geleverd wordt, wordt de beslistermijn verlengd.

6. Formeel gezien is het onderzoeksbeleid gemandateerd aan directeur van het Instituut voor Informatica, die verantwoordelijk is voor zowel het onderzoeksniveau als de wetenschappelijke oriëntatie van het instituut. Hij dient op basis van het advies van de ECIS te besluiten. Dit besluit valt onder het bestuursrecht, met de daarbij behorende bezwaarprocedures.

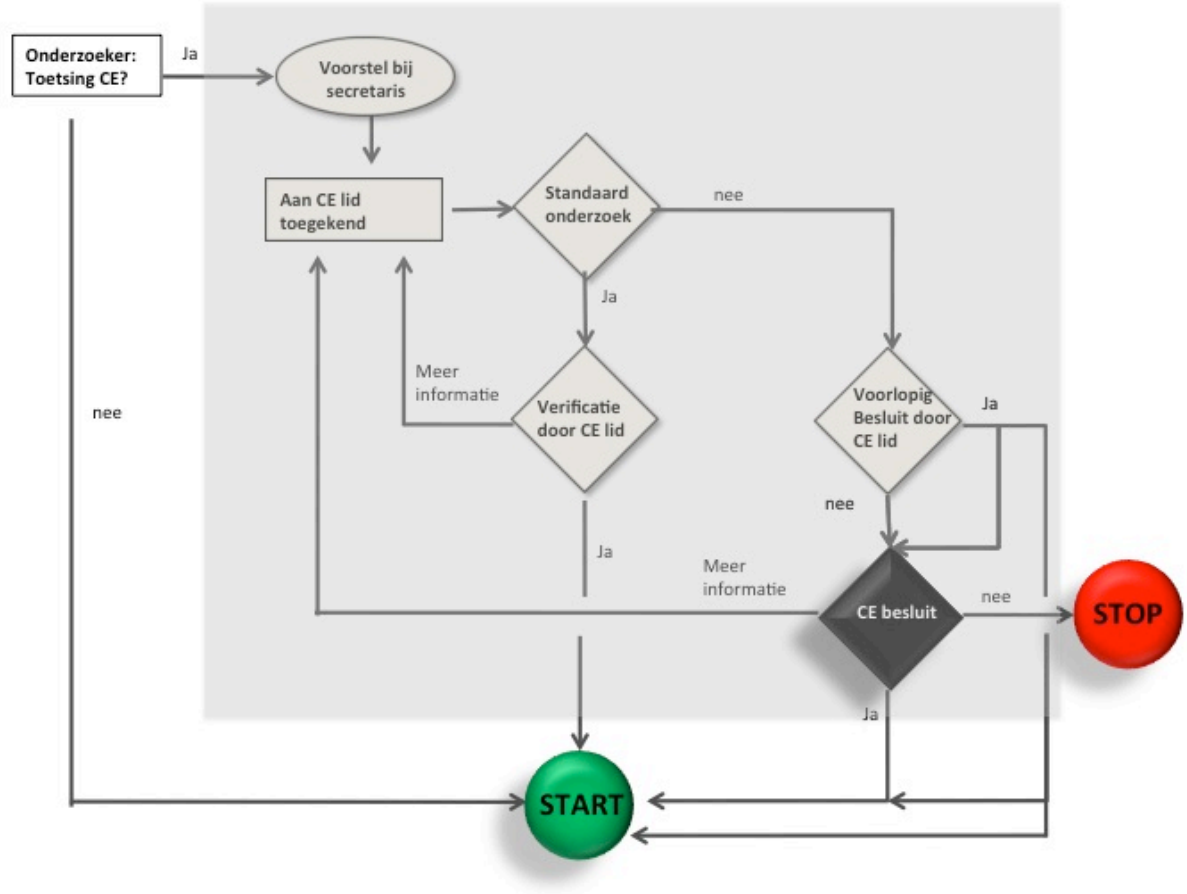
* Huidige samenstelling van de commissie is/Leden van ECIS:
Voorzitter: M. Worring
Vice-voorzitter: C. T.A.M. de Laat
Secretaris: J. van der Ham
Jurist: M.C.L. Leenen
Overige leden: H.A. Afsarmanesh, J.A. van Ginkel, F.A.H. van Harmelen, J. Heringa, P. S.Cesar, J.R. van Ossenbruggen

Procedure voor het indienen van een onderzoekvoorstel[1]

1. Voor een goede beoordeling van het onderzoeksproject is het van belang dat u weet bij welke sectie een bepaald type onderzoek zal worden uitgevoerd. Het uiteindelijke oordeel over bij welke sectie een onderzoek geacht wordt te worden uitgevoerd ligt bij het bij de betreffende sectie behorende ECIS lid. Vaak hebben onderzoekers binnen een sectie al ruime ervaring met een bepaald type onderzoek. Onderzoek dat nog nooit bij een bepaalde sectie is uitgevoerd zal eerder nadere aandacht van de ECIS behoeven.

Zie Appendix I voor een omschrijving van de verschillende secties en bijbehorend Standaard onderzoek.

2. Vul de checklist in (zie Appendix II). Eerst dient het algemene gedeelte te worden ingevuld, daarna het gedeelte dat hoort bij de sectie waar het onderzoek zal worden uitgevoerd.
De vragen van de checklist dienen uiteraard naar waarheid te worden ingevuld. Ook wordt uitdrukkelijk gevraagd de vragen te beantwoorden naar de geest van de tekst en niet zozeer naar de letter. Met andere woorden, het is niet de bedoeling om een mogelijk onduidelijke formulering naar eigen voordeel te interpreteren. Zelfs in geval van geringe twijfel dient altijd bij het antwoord 'twijfel' te worden aangevuld. Dit geldt met name voor het beantwoorden van de vraag of uw onderzoek binnen een bepaalde standaard categorie valt. Het is uiteraard onmogelijk om alle mogelijke versies van een bepaald onderzoek te voorzien, dus deze beschrijvingen zullen daardoor nooit volledig zijn. Stel alleen dat uw onderzoek tot een Standaard onderzoek behoort als inderdaad aan alle voorwaarden die in de omschrijving gesteld zijn voldaan is. Ook hier dient bij de geringste twijfel bij het antwoord 'twijfel' te worden ingevuld.



[1] Markham, A., & Buchanan, E. (2012). Ethical decision-making and Internet research: Recommendations from the AOIR ethics working committee (version 2.0). Available at http://www.aoir.org/reports/ethics.pdf.

figuur 1. Flowchart indienen van onderzoek-voorstel.

Aan het einde van de checklist blijkt of uw onderzoek een verkorte procedure bij de ECIS kan doorlopen (3a), dan wel dient te worden voorgelegd (3b).

3a. In geval van een verkorte procedure kunt u volstaan met het opsturen van de checklist en de bijbehorende documenten aan de secretaris van de ECIS. Na ontvangstbevestiging zal uw aanvraag worden doorgestuurd naar een ECIS lid met de juiste expertise. Deze zal u rechtstreeks (per e-mail) berichten over het resultaat en tevens een afschrift daarvan naar de secretaris sturen.

3b. In het geval dat het onderzoek moet worden voorgelegd aan de ECIS, dient u een beknopte omschrijving van het onderzoek (beperkt tot die aspecten die ethisch relevant zijn) naar de secretaris van de ECIS te sturen. In die omschrijving dient in ieder geval duidelijk te worden gemaakt op welke punten het onderzoek afwijkt van 'standaard' onderzoek. Indien het onderzoek wel standaard is bij een andere sectie dan de sectie waar het onderzoek wordt uitgevoerd, kan hiernaar worden verwezen in de betreffende omschrijving.

In alle gevallen wordt het voorstel door het ECIS lid van de relevante sectie gemeld aan de ECIS als geheel. De ECIS kan besluiten om hierover een ad-hoc vergadering te organiseren of om het voorstel te bespreken op de eerstvolgende geplande ECIS vergadering. De relevante portefeuillehouder kan echter in sommige gevallen in de tussentijd wel voorlopige toestemming geven voor de start van het onderzoek. Deze eventuele toestemming is dus voorwaardelijk en pas nadat de ECIS zich heeft beraad over dit onderzoek kan definitieve* goedkeuring worden verleend. Indien geen goedkeuring wordt gegeven, zullen de redenen hiervoor bekend worden gemaakt en eventuele suggesties voor verbetering gegeven worden.

* Het kan voorkomen dat een lopend onderzoek in de toekomst alsnog aspecten blijkt te hebben die een uitspraak van de ECIS vereisen. In dit geval moet dit onmiddellijk gemeld worden en in overleg met de secretaris dient bepaald te worden of onmiddellijke actie nodig is.

Procedure voor het uitvoeren van een onderzoeksproject[2]

Juridische aspecten[3]

De ontdekker van een kwetsbaarheid is in eerste instantie verantwoordelijk voor zijn of haar eigen handelen en dus de middelen waarmee hij/zij de kwetsbaarheid ontdekt heeft. Het melden van de kwetsbaarheid garandeert niet dat de ontdekker, indien hij bij het aantonen van de kwetsbaarheid een strafbaar feit heeft gepleegd, niet vervolgd wordt, maar maakt de kans op strafrechtelijk onderzoek wel kleiner.

De kans op een strafrechtelijk onderzoek en vervolging wordt nog kleiner als de ontdekker zich niet juridisch kwetsbaar heeft opgesteld door zich aan de volgende richtlijnen te houden:

- Maak geen gebruik van social engineering om op die wijze toegang te verkrijgen tot het systeem. Social engineering is een techniek waarbij een computer kraker een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de beveiliging, namelijk de mens, te kraken. De aanval is erop gericht om vertrouwelijke of geheime informatie los te krijgen, waarmee de hacker dichter bij het aan te vallen object kan komen.

- Plaats geen eigen backdoor in een informatiesysteem om vervolgens daarmee de kwetsbaarheid aan te tonen. Daarmee kan namelijk aanvullende schade worden aangericht en worden er vaak onnodige veiligheidsrisico's gelopen.

- Maak niet meer misbruik van een kwetsbaarheid dan noodzakelijk is om de kwetsbaarheid vast te stellen.

- Kopieer, wijzig of verwijder geen gegevens in het systeem. Een alternatief hiervoor is het maken van een directory listing.

- Breng geen veranderingen in het systeem aan.

- Probeer niet herhaaldelijk toegang tot het systeem te verkrijgen of deze toegang te delen met anderen.

- Maak geen gebruik van het zogeheten "bruteforcen" van toegang tot systemen. Daarbij is immers geen sprake van een kwetsbaarheid, maar alleen van het herhaaldelijk proberen van wachtwoorden.

[2] E.g. Swiss Informatics Society, code of ethics

[3] '**Leidraad** om te komen tot een praktijk van *Responsibe Disclosure*', 2013, *Ministerie van Veiligheid en Justitie*

Procedure voor het publiceren van een onderzoek

Responsible Disclosure[4,5]

In het geval van het vinden van een zwakheid in een systeem, behoeft met name het proces rondom het informeren van de systeemeigenaar regie, omdat dit een delicaat proces met wederzijds grote belangen is. Potentiële schade indien de methode in verkeerde handen valt (of al is), reputatie schade en de mogelijkheid voor studenten hun werk te publiceren zijn voorbeelden van deze belangen.

De meest gangbare manier om met de betreffende organisatie te communiceren is met de reponsible disclosure methode. Dit is een full disclosure, maar de benadeelde partij wordt tijd gegeven om de zwakke plek te dichten voordat de informatie gepubliceerd wordt. De hoeveelheid tijd en mate van disclosure hangt af van de potentiële impact.

Er worden drie fasen onderscheiden:

Onderzoeksfase

In deze fase wordt de zwakke plek gevonden. Indien de gebruikte methode niet juridisch en ethisch correct is, moet de ernst van de afwijking van de methode worden bepaald. Bij studentenonderzoek, is de begeleidende docent hier verantwoordelijk voor. In geval van twijfel dient er juridisch advies te worden ingewonnen. In de tussenliggende periode moet alles vertrouwelijk blijven en geldt er een geheimhoudingsplicht.

Communicatiefase:

Voordat de bevindingen gepubliceerd kunnen worden, moet de andere partij volledig op de hoogte zijn van het probleem en de daar bijhorende risico's. Dit is de verantwoordelijkheid van de ontdekker/melder (zie voorbeeld). Indien nodig kan er een derde partij worden ingeschakeld. Deze communicatie moet indien mogelijk vertrouwelijk van aard zijn om vroegtijdig lekken te voorkomen.

Vervolgens moet de benodigde hersteltijd worden vastgesteld. Dit gebeurt in overleg, maar 30 dagen is in de praktijk gangbaar. Ook de mate van vertrouwelijkheid dient te worden vastgesteld en afhankelijk van het belang dient de kenniskring te worden bepaald. Tijdens deze fase moet volledig open kaart worden gespeeld en moet alle benodigde informatie om de zwakke plek te reproduceren ter beschikking gesteld worden.

Alle stappen in de communicatiefase moeten worden vastgelegd in een proces verbaal ter dossier vorming en evaluatie achteraf.

Eindfase

Indien de partijen samen hebben vastgesteld dat het probleem is opgelost, mag de informatie gepubliceerd worden.

Zie appendix III voor een voorbeeld van een concreet plan van aanpak.

[4] website marktplaats.nl

[5] 'Vulnerability Disclosure, How do we define Responsible Disclosure?', Stephen A. Shepherd, 2003, SANS Institute

Appendix I

Deze appendix kent een autonome ontwikkeling en krijgt in de tijd vorm.

Appendix II

Generieke vragen

Algemeen

1. Titel van het project
2. Verantwoordelijke onderzoeker (ook HL bij promotie)
3. Uitvoerende onderzoekers
4. Hoogleraar-stoel
5. Plaats van uitvoering van het onderzoek
6. Korte omschrijving van het project
7. Namen van betrokken organisaties
8. CE lid van betreffende leerstoel

Vragen

1. Heeft u dit of soortgelijk onderzoek al eerder ingediend bij de CE?

☐ Ja
☐ Nee

2. Zijn er externe objecten betrokken bij het onderzoek?

☐ Ja
☐ Nee

zo ja, zijn de objecten van participerende onderzoek partners?

3. Is de eigenaar van het object op de hoogte van het gebruik?

☐ Ja
☐ Nee

Zo nee, waarom niet?

4. Is er juridisch advies ingewonnen?

☐ Ja
☐ Nee

Zo ja, advies graag bijsloten.

5. Zijn er disclosers afgesloten?

☐ Ja
☐ Nee

Zo ja, met wie en waarover?

6. Is het onderzoek publicitair gevoelig?

☐ Ja
☐ Nee

Zo ja, kan je in het kort de gevoeligheid schetsen?

De volgende vragen is een goed startpunt om de ethische aspecten te beschouwen. Zie voor een toelichting; Markham, A., & Buchanan, E. (2012). Ethical decision-making and Internet research: Recommendations from the AOIR ethics working committee (version 2.0). Available at http://www.aoir.org/reports/ethics.pdf.

Specifieke vragen

Commercial web services (data storage)

1. What are the participant/author's expectations of privacy?
2. Is the data easily searchable and retrievable? Is the data subject to open data laws or regulations?
3. Does the service's privacy policy contradict ethical principles?
4. What measures safeguard data at the site of data collection?
5. How long will the data be stored on the servers?
6. Does this contradict the time frame indicated by the researcher or institutional policies?
7. What happens to the data after the researcher completes work on the service?
8. How are the data destroyed?
9. How will cross---border data be handled if IP addresses are considered by one country to fall under privacy regulations?

Databanks

10. Where is the data stored?
11. How long will the data exist in the repository?
12. What consent is needed for subsequent data use?
13. Does the remixing/mashing of data enable identification of individual or group identities or enable any additional risks to participants?
14. In the case of shared data, what conditions were placed on data use by the original researcher, if any?

15. Regardless of conditions, what ethical responsibilities may require consideration by later users?
16. What mechanisms are in place to ensure appropriate data provenance and ownership?
17. How will images/audio be effectively anonymized?

Security

18. Are you searching for a vulnerability in a network or application?
19. Does the owner of the information system knows you are searching for vulnerability?
20. Are the activities in conflicts with regulations?
21. Which law applies? Dutch, American……?
22. What is the impact of the vulnerability?
23. Does the vulnerability affects anyone privacy ?
24. How do you communicate with the owner of the vulnerability?
25. How can researcher ensure that author/participant understands and agrees that content or interaction may be used for research purposes?
26. Is the communication archived or easily searchable and retrievable?
27. Is the data subject to open data laws or regulations?
28. How long does the third party provider or ISP preserve the data and where?
29. Could privacy be achieved through anonymization of email content and/or header information?

Special interest forums

30. How do terms of service (TOS) articulate privacy of content and/or how it is shared with 3rd parties?
31. Regardless of TOS, what are community or individual norms and/or expectations for privacy?
32. Does the author/subject consider personal network of connections sensitive information?
33. Is the data easily searchable and retrievable?
34. If the content of a subject's communication were to become known beyond the confines of the venue being studied – would harm likely result?
35. Is the conversation thread or forum perceived as public or private by the author(s)/subject(s)?
36. How is profile, location, or other personally identifying information used or stored by researcher?

37. Is the data easily searchable and retrievable?

38. How is informed consent or protection of privacy achieved?

39. How are vulnerable persons identified and protected?

40. If non---active archives are used, how is vulnerability or harm defined and how are potential or actual subjects protected?

Social networking

41. How do the terms of service articulate privacy of content and/or how it is shared with 3rd parties?

42. Does the author/participant consider personal network of connections sensitive information?

43. How is profile or location information used or stored by researcher?
    Does author/participant understand and agree to interaction that may be used for research purposes?

44. Does research purpose and design balance possible conflicts between participant and researcher perceptions of public/private and sensitive/nonsensitive?

45. Does the dissemination of findings protect confidentiality?

46. Is the data easily searchable and retrievable?

47. If the content of a subject's communication was ever linked to the person, would harm likely result?

Personal spaces

48. Could analysis, publication, redistribution, or dissemination of content harm the subject in any way?

49. If the content of a subject's communication were to become known beyond the confines of the venue being studied would harm likely result?

50. Does the author/participant consider personal network of connections sensitive information?

51. Does author/participant consider the presentation of information or venue to be private or public?

52. Do the terms of service conflict with ethical principles?

53. Is the author/subject a minor?

Virtual worlds

54. Should these virtual worlds be considered "public"?

55. What constitutes "privacy" in such places?

56. Should avatars be considered as persons and afforded the same protections as human subjects?

57. Will the process of requesting consent itself cause harm?

58. How and when should consent be sought?

59. What requires consent?

60. To what extent do users perceive their interactions and communication to be private in these spaces?

61. How do Terms of Service specify researcher presence, anonymity of users, and privacy/ confidentiality?

62. To what extent and in what ways could research activities interfere with or compromise a user's play or outcomes in the game?

63. How should researchers juggle their own multiple roles?

64. Could data be used to identify a user's physical location and other sensitive demographic information?

Appendix III

Voorbeeld eerste communicatie

Geachte heer/mevrouw,

In de afgelopen twee weken is er in het kader van de universitaire master-opleiding System & Network Engineering aan de Universiteit van Amsterdam onderzoek gedaan naar de veiligheid van verschillende mobiele applicaties, waaronder die van X.

Dit onderzoek is uiterst zorgvuldig gedaan met in achtneming van de wet- en regelgeving conform de richtlijnen van het Nationaal Cyber Security Center (NCSC).

Uit dit onderzoek is een aantal zaken naar voren gekomen die uw aandacht vereisen. Wij denken een zwakke plek gevonden te hebben in uw applicatie voor Android waardoor de persoonlijke gegevens..... De resultaten zijn nog vertrouwelijk.

Graag willen wij deze resultaten aan u presenteren zodat u stappen kunt ondernemen om de problemen op te lossen, voordat wij deze informatie publiceren. Het is hierbij onze intentie om te handelen volgens de 'Leidraad om te komen tot een praktijk van Responsible Disclosure' van de NCSC.

Wij verzoeken u daarom spoedig contact met ons op te nemen door te reageren op deze e-mail.

Met vriendelijke groet,

melder

Plan van aanpak bij het vinden van een kwetsbaarheid

1. Er dient een proces coördinator (PC) te worden aangewezen door de voorzitter van het IvI. Gegeven de benodigde inhoudelijke kennis, slagvaardigheid en diplomatie moet gedacht worden aan een senior staflid. Hij/zij moet het proces bewaken en stimuleren en het bevoegd gezag binnen de instelling op de hoogte brengen. Gedurende het proces heeft de PC de regie en alle acties (inclusief publicitaire) dienen toestemming van de PC te krijgen.

2. Er moet vastgesteld worden of het onderzoek juridisch- en ethisch verantwoord was. (actie PC i.o.m. jurist)

3. Er dient een brief te worden geschreven over de feitelijke bevindingen met daarin tevens een voorstel tot responsible disclosure. Dit kan getrapt gebeuren.

    a.Operationeel niveau. (actie: docent)

    b.Op tactisch en strategisch niveau. (actie: hoofd opleiding)

Diegene kan worden bijgestaan door een jurist en eventueel een communicatieadviseur. De laatste kan bewaken dat de brief welluidend en zakelijk is.

4. Indien de zorgvuldigheid dat vereist moet de brief worden voorgelegd aan de decaan van de FNWI voordat deze naar de organisatie gaat.

5. Publicatie onderzoeksresultaten. Voor interne doeleinden dient er een populaire (dus begrijpelijk voor niet-informatici) versie van het onderzoeksverslag te zijn.