Ethik in der Sicherheitsforschung

Sebastian Schrittwieser[1] · Martin Mulazzani[2] · Edgar Weippl[2] · Sandra Panhans[2]

[1]Technische Universität Wien
sebastian.schrittwieser@tuwien.ac.at

[2]SBA Research
{mmulazzani,eweippl,spanhans}@sba-research.org

Zusammenfassung

In letzter Zeit wurden zahlreiche Forschungsarbeiten im Bereich der Informationssicherheit veröffentlicht, die als unethisch betrachtet werden könnten. Es ist wichtig einen Blick auf diese Grenzfälle zu werfen, da die heutigen Forschungsarbeiten einen Einfluss darauf haben werden, wie junge Forscher ihre Forschung betreiben werden. Im vorliegen Artikel diskutieren wir grundlegende ethische Prinzipien und deren Rolle in der aktuellen Literatur. Wir argumentieren dahingehend, dass die Schaffung ethischer Richtlinien oder Rahmenbedingungen ohne vorherige Diskussion und Einigung innerhalb der wissenschaftlichen Gemeinschaft wahrscheinlich nicht zur Klarheit führen wird, welche Grenzen in der wissenschaftlichen Forschung nicht überschritten werden sollten.

1 Einleitung

In letzter Zeit kann eine neue Entwicklung in der Informationssicherheitsforschung beobachtet werden. Es gibt zahlreiche aktuelle Artikel, die wichtige Sicherheitsfragen quantitativ analysieren (z.B. [KKL+09], [SCC+09], [JJJM07], [BSBK09], [MBG+08]). Während viele frühere Arbeiten Gefahren theoretisch betrachteten (z.B. die berühmte Arbeit „Trusting Trust" [Thom84] von 1984), würden heutige Forscher ihre Forschung wahrscheinlich durch die Ausführung eines Angriffs und dessen Evaluierung „in freier Wildbahn" validieren. Dieser Trend rührt zu einem gewissen Grad sicherlich von mehreren bedeutenden Paradigmenwechseln her, denen wir in der heutigen technologischen Welt gegenüber stehen. Daten wandern von lokalen Datenspeichern zu dezentralisierten Diensten im Internet, große Mengen an benutzergenerierten Inhalten werden in sozialen Netzwerken speichert, etc. Vereinigt unter dem Begriff „Big Data", führen diese grundlegenden Änderungen im Umgang mit Technologie zu einem neuen Forschungstrend, der reale Personen und reale Daten direkt beeinflusst.

Ethische Konsequenzen sind in diesem Forschungsfeld offensichtlich und betreffen zwei Bereiche. Zum einen müssen wir immer darüber nachdenken, wie Forschungsergebnisse missbraucht werden könnten. Eine Zeile aus einem satirischen Lied über Wernher von Brauns Einstellung gegenüber den Konsequenzen seiner Arbeit an den V2-Raketen in Nazi-Deutschland besagt „*Once the rockets are up, who cares where they come down? / That's not my department*". Wernher von Braun war an der Erforschung von Raketentechnologie interes-

siert und nahm hin, dass die Ergebnisse seiner Arbeit für die Entwicklung von Waffen genutzt wurden. Vergleichbar damit, müssen wir abschätzen, wie unsere Forschung missbraucht werden könnte. Berücksichtigt die Entwicklung von Analysemethoden für Anonymisierungsnetzwerke wie Tor [MBG+08], die ethischen Konsequenzen der Möglichkeit, dass gewaltsame Regime die Forschungsergebnisse zur Deanonymisierung von Bürgen verwenden und diese verfolgen könnten?

Zum anderen müssen wir gewährleisten, dass unsere Forschungsaktivitäten selbst niemand anderem Schaden zufügen. Obwohl die möglichen Folgen gewiss nicht derart wesentlich für die Menschheit sind, wie beispielsweise Stammzellenforschung oder andere naturwissenschaftliche Belange, verspüren wir das Bedürfnis uns mit ethischen Fragen zu befassen. Ein wichtiger Grund hierfür ist, dass die persönliche Moral von Sicherheitsforschern den kritischen Faktor zwischen *white* und *black hats* darstellt; wir müssen festlegen, wie weit wir in der Forschung gehen können. Für Forscher im Bereich der Informationssicherheit besteht der jüngste Erfolg von Artikeln wie den obengenannten darin, dass sie einen Anreiz haben, ihre Forschung weiterhin auf diese Art und Weise durchzuführen.

In der vorliegenden Arbeit, wollen wir uns auf die zuletzt genannte Art von ethischen Auswirkungen konzentrieren und beabsichtigen eine Diskussion darüber anzuregen, wie wir Forschungsaktivitäten im Bereich der Informationssicherheit von einem ethischen Standpunkt aus evaluiert können und wie wir als wissenschaftliche Gemeinschaft ethische Standards, vergleichbar zu solchen in der medizinischen Forschung, etablieren können.

1.1 Literatur

In diesem Abschnitt stellen wir vier unserer Meinung nach umstrittene Artikel und ihre ethischen Überlegungen vor und diskutieren diese. Wir wollen hervorheben, dass alle Artikel die Freigabe einer Ethikkommission erhalten haben und es zweifellos nicht unsere Absicht ist, die Autoren für ihre Forschung zu kritisieren. Ihre Artikel sollen lediglich als Beispiele für kontrovers diskutierte Forschung dienen.

1.1.1 Spamalytics – An empirical analysis of spam marketing conversion [KKL+08]

Die Grundidee dieses Forschungsprojekts bestand darin, die Wirtschaftlichkeit eines Botnetzes zu untersuchen, das dazu verwendet wurde, täglich Millionen von Spamnachrichten zu versenden. Die Forscher brachen zu diesem Zweck in ein Botnetz ein, analysierten es und manipulierten einen kleinen Prozentsatz der Nachrichten derart, dass die Handlungen der Adressaten, wie zum Beispiel das Klicken auf Links, für die Forscher analysierbar waren. Die Autoren argumentierten, dass ihre Forschung ethisch korrekt sei, weil sie sich lediglich als „*passive actors*“ sahen, die „*neutral actions*“ gewährleisteten und da Betroffenen niemals zusätzlicher Schaden zugefügt wurde („*users should never be worse off due to [their] activities*“).

1.1.2 Your Botnet is My Botnet: Analysis of a Botnet Takeover [SCC+09]

Dieser Artikel beschreibt die Übernahme eines Botnetzes für Analysezwecke. Die Autoren waren sich darüber im Klaren, was der Einbruch in den Command & Control Server eines Botnetzes für ethische Konsequenzen nach sich zieht und brachten die folgenden Argumente:

- *„The sinkholded botnet should be operated so that any harm and/or damage to victims and targets of attacks would be minimized“*
- *„The sinkholded botnet should collect enough information to enable notification and remediation of affected parties“*

1.1.3 Pharmaleaks – understanding the business of online pharmaceutical affiliate programs [MPJ+12]

In diesem Artikel wurde die Datenbank eines Onlinehändlers für pharmazeutische Produkte analysiert, welche aus einem früheren Angriff auf dessen Infrastruktur stammte. Zum Zeitpunkt der Untersuchung waren die Daten bereits im Internet veröffentlicht, sodass die Forscher diese Tatsache heranziehen konnten, um ihre Analysen zu rechtfertigen:

- *[…] ethics of using data that was, in all likelihood gathered via illegal means. […] We justify our own choice […] by reaoning about harm.“*
- *„some […] contents have already been widely and publicly documented. Consequently, we cannot create any new harm simply through association with these entitites or repeating these findings“*

1.1.4 Is the Internet for Porn? An Insight Into the Online Adult Industry [WHP+10]

Die Autoren dieses Artikels analysierten die Wirtschaftlichkeit von sogenannten „Traffic trading“-Netzwerken für Webseiten mit pornographischem Inhalt und nahmen sogar selbst mit einer eigenen Webseite am Netzwerk teil. Ethische Überlegungen wurden folgendermaßen erörtert:

- *„Clearly, one question that arises is if it is ethically acceptable […] to participate in adult traffic trading. […] we believe that realistic experiments are the only way to reliably estimate success rates of attacks in the real-world“*
- *„we did not withdraw any funds but forfeited our traffic trading accounts at the end of the experiments“*

1.2 Grundlegende Prinzipien

Auf den ersten Blick scheinen alle vorgetragenen Argumente zur ethischen Rechtfertigung der vorgestellten Forschungsprojekte gültig und angemessen. Im Rahmen dieser Arbeit wollen wir grundlegende ethische Prinzipien diskutieren und diese mit den Artikeln und deren Ar-

gumentation bezüglich der Forschungsethik vergleichen. Die Grundsätze folgen keinen speziellen ethischen Richtlinien, noch wurden sie von anderen wissenschaftlichen Fachgebieten wie der Medizin übernommen. Wir haben vielmehr versucht, die grundsätzlichsten Prinzipien aus dem gesunden Menschenverstand abzuleiten. Der Hintergedanke dabei ist, dass wir fest davon überzeugt sind, dass ohne einen allgemeinen Konsens über die fundamentalsten Grundlagen von ethischen Forschungsmethoden in der Informationssicherheit, die Definition von zu detaillierten Richtlinien und Rahmenbedingungen keine Akzeptanz unter den Forschern finden würde.

1.2.1 Füge Menschen nicht absichtlich Schaden zu

Ein scheinbar einfaches Prinzip besteht darin, dass Forscher anderen Personen nicht aktiv Schaden zufügen dürfen. Zum Beispiel ist es offenkundig eine schlecht Idee seine eigene Malware zu schreiben, um damit Infektionszahlen und verschiedene Ausbreitungsstrategien zu studieren. Die Vergangenheit hat allerdings gezeigt, dass in anderen wissenschaftlichen Bereichen selbst naheliegend scheinende Prinzipien verletzt wurden. Eine der wichtigsten ethischen Fälle in der medizinischen Forschung, ist die sogenannte Tuskegee-Syphilis-Studie[1]. Die 1932 gestartete Studie zielte darauf ab, die Verbreitung und mögliche Behandlungen von Syphilis zu untersuchen. 1947 wurde festgestellt, dass sich Penicillin für die Behandlung von Syphilis eignet. Nichtsdestotrotz dauerte das Experiment weitere 25 Jahre an, bevor es in den 70er-Jahren aufgrund öffentlichen Drucks beendet wurde. Während der 40-jährigen Laufzeit wurden Patienten nicht über verfügbare Behandlungen informiert, es wurden keine Vorsichtsmaßnahmen getroffen, damit sie keine anderen Personen infizieren und ihnen wurden zudem bewusst falsche Informationen bezüglich der Behandlung gegeben. Heute ist es offensichtlich, dass eine solche Studie unethisch ist. Ärzten ist es nicht nur nicht gestattet Informationen über wirksame Behandlungen zurückzuhalten, sondern sie müssen Patienten auch das Studiendesign erläutern. Im Zuge von randomisierten Doppelblindstudien kann weder der Arzt, noch der Patient darüber entscheiden, ob ein Patient ein neues, möglicherweise besseres Medikament erhält oder die Standardbehandlung. Niemand würde dem Patienten die Standardbehandlung vorenthalten, wie dies in der Tuskegee-Studie der Fall war.

In der medizinischen Forschung sind heute die Grenzen, die nicht überschritten werden dürfen, eindeutig festgelegt (wie z.B. in der Deklaration von Helsinki [KiWM09]) und mögliche Auswirkungen von unethischen Studien sind durch eine große Anzahl an Forschungsskandalen hinreichend bekannt: Medizinische Forschung wirkt sich direkt auf das menschliche Leben aus. Die Auswirkungen von Informationssicherheitsforschung können wohl nicht mit der medizinischen Forschung verglichen werden. Allerdings haben mehrere Fälle im Verlauf der vergangen Jahre gezeigt, dass sie dennoch einen drastischen Einfluss auf beteiligte Personen haben können. Obwohl es sich nicht um wissenschaftliche Forschung handelt, hat das „Craigslist Experiment“[2] auf eine sehr drastische Weise die Auswirkungen von unethischer Forschung gezeigt und es ist zweifelsfrei möglich, sich vorzustellen, dass in wissenschaftlichen Studien mit einem ähnlichen Aufbau Verhalten, das die Privatsphäre von anderen Menschen beeinflusst (wie z.B. [Inte07]), oder Cyber-Mobbing in einem sozialen Netzwerk untersucht wird.

[1] http://de.wikipedia.org/wiki/Tuskegee-Syphilis-Studie

[2] http://en.wikipedia.org/wiki/Jason_Fortuny#.22Craigslist_Experiment.22

Ein weiterer problematischer Aspekt besteht in unvorhersehbaren Auswirkungen auf die analysierten Systeme. Es gestaltet sich oft schwierig, den Einfluss von Handlungen, die für Forschungszwecke ausgeführt werden, abzuschätzen und Schaden kann selbst dann entstehen, wenn dieser nicht beabsichtigt war. Ein Botnetz ist beispielsweise ein komplexes und in den meisten Fällen undokumentiertes System. Wie können Analysen durchgeführt werden, während zugesichert wird, dass die ausgeführten Maßnahmen das Systems und dessen unfreiwilligen Teilnehmer nicht auf eine schadhafte Weise beeinflussen?

1.2.2 Schaue nicht zu wie schlimme Dinge passieren

Nicht zuzusehen, wie schlimme Dinge passieren, ist das zweite Prinzip. Im echten Leben gibt es den Ausdruck „unterlassene Hilfeleistung“. Wenn man beispielsweise Zeuge eines Verkehrsunfalls mit verletzten Personen wird, hat man die gesetzliche Verpflichtung Erste Hilfe zu leisten. Auf den ersten Blick erscheint dieses Prinzip ebenso einleuchtend wie das erste. Allerdings zeigt eine Betrachtung der zuvor behandelten Artikel, wie schwierig es zu befolgen ist.

Die Autoren des „Spamalytics“-Papers [KKL+09] argumentierten damit, lediglich „*passive actors*“ zu sein und „*neutral actions*“ zu gewährleisten. Es ist richtig, dass die Forschungsaktivitäten keinem Benutzer aktiv Schaden zufügten (das erste Prinzip). Ferner argumentierten die Autoren, dass sie mit der Manipulation einiger Spamnachrichten zumindest ein wenig Gutes für einige der Empfänger der Spamnachrichten getan haben. Jedoch ist genau das der entscheidende Punkt. Die Forscher verhinderten nicht, dass dennoch Millionen der echten Spamnachrichten über das Botnetz versendet wurden und diese Netzbetreibern und Mailinfrastrukturen Schaden zufügten. Den Forschern war bekannt, welche Computer infiziert waren, aber sie schauten ohne zu helfen zu. Man könnte argumentieren, dass Spam ein lästiger Bestandteil der heutigen E-Mail-Kommunikation ist, welchem die meisten Benutzer aber nicht viel Aufmerksamkeit schenken. Es sollte jedoch nicht vergessen werden, dass es dennoch eine große Anzahl an Personen gibt, die auf diese Nachrichten hereinfallen – ansonsten würde sich das Spam-Geschäft nicht für den Sender auszahlen. Ein Bericht von Commtouch aus dem Jahr 2012 [Comm12] zeigt, dass nach wie vor 50 Prozent der weltweit versendeten Spamnachrichten Arzneimittel oder andere medizinische Produkte bewerben, welche zu einem großen Prozentsatz gefälscht sind und ein großes Gesundheitsrisiko darstellen. Wenn der Versand von Spamnachrichten verhindert wird – und die Möglichkeit bestand in diesem Forschungsprojekt –, könnten Menschen davor geschützt werden gefährliche Medikamentenfälschungen zu bestellen.

In [SCC+09] argumentierten die Autoren, dass sie den Schaden für die Opfer minimiert hätten („*damage to victims […] would be minimized*“). Das Problem jedoch ist, dass es schwierig ist „*minimzing damage*“ zu definieren: Letztendlich würde es bedeuten, dass keine Forschung möglich ist, da die Autoren des Artikels dafür sorgen hätten müssen, dass das Botnetz abgeschaltet wird, sobald sie Zugriff darauf bekommen hatten. Die Opfer nach Beendigung des Experiments zu informieren, entspricht möglicherweise nicht dem Grundsatz von „*minimizing damage*“.

Die nächste offenkundige Frage ist, ob bestimmte Daten einfach nicht gesammelt oder diese weggeworfen werden sollten, um zu vermeiden, dass man alle Informationen zur Verfügung hat, die man benötigen würde, um Personen zu informieren. Wenn wir davon ausgehen, dass wir das letzte Beispiel (Botnetz-Analyse) als unethisch betrachten und es trotzdem durchführen, dann sollten wir zumindest die Leute kontaktieren, die von Malware geschädigt wurden

und möglicherweise nichts davon wissen. Wenn das Management jedoch entscheidet, dass es dies schlecht für das Geschäft ist, könnten wir einfach die IP-Adressen von betroffenen Geräten nicht speichern (oder löschen), aber alle anderen Daten behalten. Wir wären immer noch in der Lage unsere statistischen Analysen für das Forschungsprojekt durchführen, aber „bedauerlicherweise“ hätten wir nicht mehr die Daten zur Verfügung, um die Benutzer zu kontaktieren. Würde das (unter der bisherigen Annahme) als ethisch aufgefasst werden? Die Minimierung von Kosten und Sicherheitsanliegen könnte ein Argument dafür sein, Informationen nicht zu sammeln, da personenbezogene Daten gut geschützt werden müssen. Existierende Daten zu löschen scheint dagegen keine gute Idee zu sein.

Und selbst wenn es sowohl möglich als auch verantwortungsvoll erscheint, einen Benutzer zu informieren, dessen Computer Teil eines Botnetzes ist, könnten weitere Herausforderungen entstehen. Es könnten mehrere Benutzer eine infizierte Maschine verwenden und die Benachrichtigung eines beliebigen Benutzers, könnte zusätzlichen Schaden anrichten. Zum Bespiel könnte die Infektion eines Geschäftscomputers durch das Beenden des Antivirenprogramms, dem Surfen auf Internetseiten, die nichts mit der eigentlichen Arbeit zu tun haben, etc. verursacht worden sein. Folglich könnte die Verständigung einer Person dazu führen, dass eine andere Person ihren Job verliert.

1.2.3 Führe keine illegalen Aktivitäten durch, um illegalen Aktivitäten zu schaden

Eine andere interessante Frage ist, ob es unethisch ist, illegalen Aktivitäten Schaden zuzufügen. Nehmen wir an, eine Studie will die Effektivität abschätzen, Botnetze für den Versand von Spamnachrichten zu mieten. Es könnte für junge Forscher verlockend sein, einfach Botnetz-Ressourcen zu erwerben, um Spam zu versenden und dann zu beurteilen, wie gut die angebotene Qualität mit der tatsächlichen Performance übereinstimmt. Selbst wenn es sich bei den Empfängern nicht um echte Personen handelt, sondern um Test-E-Mail-Adressen, sodass niemandem echter Schaden durch das Versenden des Spams zugefügt wird, bleibt ein ethisches Problem bestehen: Man gibt Forschungsgelder für die Finanzierung von illegalen Aktivitäten (das Botnetz) aus. Wäre es eine vernünftige Entscheidung gestohlene Kreditkartennummern zu verwenden, um die Mietgebühr des Botnetzes zu bezahlen? Das Kreditkarteninstitut würde höchstwahrscheinlich die Zahlung widerrufen, sobald die Karte gesperrt ist und damit die Betreiber des Botnetzes ihres Einkommens berauben. Gleichwohl muss die Nutzung einer gestohlenen Kreditkarte an sich schon als unethisch betrachtet werden.

In [SCC+09] beschreiben die Autoren, wie sie in ein Botnetz eingedrungen sind, um es zu analysieren. Das Abfangen und Verändern von Nachrichten eines „legalen Botnetzs“ wie beispielsweise SETI@home[3] würden wohl die meisten Menschen als unethisch empfinden. Ist eine ähnliche Aktivität einfach nur deshalb ethisch, weil sie auf „böse“ Leute abzielt – obwohl keine Argumente zur Selbstverteidigung vorgebracht werden können? Ähnlich hierzu ist es wahrscheinlich eine schlechte Entschuldigung eines Wissenschaftlers, wenn er nach dem Einbruch in das Haus eines Diebs von der Polizei festgenommen wurde und sagt, er habe untersuchen wollen, welche Waren gestohlen wurden.

[3] http://setiathome.berkeley.edu

1.2.4 Betreibe keine verdeckte Forschung

Die Strafverfolgung hat Gesetze, die festlegen, welche Handlungen bei verdeckten Ermittlungen erlaubt sind und welche nicht und manche Ermittlungsformen benötigen die Kooperation mit der Strafverfolgung. Um Mitglied in einer kriminellen Organisation zu werden, braucht es beispielsweise oftmals eine Art von Aufnahmeritual, wie das Begehen einer Strafhandlung, um die Eignung und Loyalität einer Person auf die Probe zu stellen. In der wissenschaftlichen Forschung ist eine Kooperation mit der Strafverfolgung in vielen Ländern noch nicht gängig. Forscher, die versuchen die Marktmechanismen des lokalen Drogenhandels zu verstehen, können nicht einfach hinausgehen und Drogen zu unterschiedlichen Preisen und in unterschiedlicher Qualität verkaufen, um die Preiselastizität und Wege der illegalen Märkte zu analysieren. Neben der Gefahr von anderen Drogenhändlern erschossen zu werden, wäre ihre Forschung gesetzeswidrig. Ebenso kann das „Testen" von illegalen Märkten durch den Kauf von Botnetzes und gestohlenen Kreditkartenummern als unethisch betrachtet werden, weil Kriminelle Geld dabei verdienen.

In [WHP+10] argumentierten die Autoren, dass sie auf verdeckte Forschung angewiesen waren („*... believe that realistic experiments are the only way to reliably estimate succes rates of attacks in the real-world*"). Jedoch löst diese Argumentation nicht das ethische Dilemma. „Wir mussten auf diese Weise handeln" ist niemals ein gutes Argument in der wissenschaftlichen Forschung. Niemand zwingt einen Forscher dazu ein bestimmtes Experiment durchzuführen. Das vorgestellte Forschungsprojekt ist ganz eindeutig verdeckte Forschung, welche zumindest zu problematischen ethischen Sachverhalten führen könnte.

2 Diskussion

Auf der einen Seite sind der wissenschaftlichen Gemeinschaft der Informationssicherheitsforschung die ethischen Fragen innerhalb ihres Feldes wohl bekannt. Die meisten Artikel, die sich mit großen Mengen an personenbezogenen Daten oder dem Einbruch in Systeme befassen, beinhalten einen Ethik-Abschnitt und zumindest an U.S.-amerikanischen Universitäten gibt es Ethikkommissionen, bei denen Wissenschaftler ihre Anträge überprüfen lassen müssen. Erst kürzlich hat die Europäische Union eine optionale Prüfungskommission für das Forschungsrahmenprogram FP7[4] vorgestellt, das zum Teil mit den Ethikkommissionen in den USA vergleichbar ist. Auf der anderen Seite hat der Vergleich jedoch gezeigt, wie schwierig es ist, auch nur die grundlegendsten ethischen Prinzipien zu erfüllen. Die Frage, die daraus hervorgeht ist, wie wir, die wissenschaftliche Gemeinschaft der Sicherheitsforschung, eine zufriedenstellendere Situation erreichen können. Kann der Vorschlag eines ethischen Rahmenwerks dazu beitragen, Forschungsideen in Anbetracht ethischer Aspekte leichter bewertbar zu machen? Wir sind zumindest skeptisch, was dies anbelangt.

Ein Grund dafür ist, dass sich die Dinge in der Informationstechnologie schnell ändern – deutlich schneller als in anderen Bereichen. Wir vermuten, dass die Gefahr besteht, Richtlinien zu etablieren, die nicht das aktuelle technologische Umfeld widerspiegeln. Ein Blick auf die jüngste Geschichte der medizinischen Forschung zeigt das Dilemma. Jede neu entwickelte Forschungsmethode bringt neue ethische Fragen mit sich, die – in einigen Fällen – Jahre an Diskussion in der Gesellschaft und darüber hinaus (z.B. Politik, Religion etc.) zur Folge ha-

[4] http://www.surveilleadvisoryservice.eu

ben. Eines der bekanntesten Beispiele der letzten Jahre ist die Stammzellendebatte, welche vor 15 Jahre mit einer bahnbrechenden Arbeit von Thomson et al. [TIS+98] begann. Die Debatte hält bis heute an, ohne dass ein allgemeiner Konsens in Sicht wäre. Klarerweise ist es schwer vorstellbar, dass Forschungsmethodologien im Bereich der Informationssicherheit einem ähnlichen Einfluss durch Politik und Religion ausgesetzt sein könnten. Sich verändernde Forschungsparadigmen durch neue technische Möglichkeiten, könnten jedoch trotzdem zu breiten und langatmigen Diskussionen führen, die die Anpassung von Richtlinien verhindern. Der Einfluss von sozialen Netzwerken auf die Privatsphäre von Nutzern wird beispielsweise heiß diskutiert und es ist unwahrscheinlich, dass die Debatte in der nahen Zukunft verebbt. Wie sollen ethische Richtlinien Forschungsaktivitäten regeln, die sich mit persönlichen Nutzerdaten in sozialen Netzwerken auseinandersetzen, wenn es darüber keinen umfassenden Konsens innerhalb der wissenschaftlichen Gemeinschaft gibt.

Ein weiteres Problem, das wir sehen, ist der Mangel an Diskussion. Im Augenblick bedeutet die Auseinandersetzung mit ethischen Fragen in den meisten Fällen, dass man eine Genehmigung einer Ethikkommission erhält und man ihnen einen Abschnitt im Artikel widmet, der die Forschung rechtfertigt. Ethische Überlegungen werden dabei oft als ein notwendiges Übel angesehen, das zwischen dem Autor und seiner Forschung steht und nicht als etwas, das als selbstverständlich betrachtet wird. Eine offenere Diskussion über ethische Aspekte unserer Forschung wäre wünschenswert. Arbeitsgruppen wie jene, aus denen der Menlo Report hervorging [DiKe11], [BDKM12] sind zweifellos ein Schritt in die richtige Richtung.

3 Zusammenfassung

Vergleichbar zu anderen Wissenschaften ist in der Informationssicherheitsforschung die Kluft zwischen dem was technisch möglich ist und dem, was von einem gesetzlichen und ethischen Standpunkt aus zulässig ist, groß. Durch diese Kluft ist es schwierig, den Platz zu finden, an dem die Grenze gezogen werden kann, die nicht überschritten werden sollte.

Wir haben versucht in diesem Artikel vier grundlegende ethische Prinzipien festzulegen, die aus naheliegenden Gründen nicht missachtet werden sollten. Ein Vergleich mit kürzlich erschienenen Forschungsarbeiten zeigt jedoch, wie schwierig es ist sie zu befolgen. Obwohl wir nicht glauben, dass die vorgestellte Literatur ethisch untragbar war (immerhin haben die Autoren die Genehmigung einer Ethikkommission erhalten), sind wir der festen Überzeugung, dass die Ergebnisse des Vergleichs zeigen, wie schwierig es ist, allgemein akzeptierte und universell gültige Prinzipien festzulegen.

Wir sind der Meinung, dass diese Fragen in der Zukunft aktiv diskutiert werden sollten und hoffentlich irgendwann zu ähnlichen Standards wie in der medizinischen Forschung und anderen Naturwissenschaften führen.

Danksagungen

Diese Forschungsarbeit wurde durch COMET K1 der FFG (Österreichische Forschungsförderungsgesellschaft) finanziert.

Literatur

[ACKL02] D. P. Anderson, J. Cobb, E. Korpela, M. Lebofsky, D. Werthimer: Seti@home: an experiment in public-resource computing. In: Communications of the ACM, ACM Vol. 45(11) (2002) 56-61.

[BDKM12] M. Bailey, D. Dittrich, E. Kenneally, D. Maughan: The menlo report. In: Security & Privacy, IEEE Vol. 10(2) (2012) 71-75.

[BEJ+09] A. L. Beberg, D. L. Ensign, G. Jayachandran, S. Khaliq, V. S. Pande: Folding@home: Lessons from eight years of volunteer distributed computing. In: Parallel & Distributed Processing, 2009. IPDPS 2009. IEEE International Symposium on., IEEE (2009) 1-8.

[BSBK09] L. Bilge, T. Strufe, D. Balzarotti, E. Kirda: All your contacts are belong to us: Automated identity theft attacks on social networks. In: Proceedings of the 18th international conference on World wide web, ACM (2009) 551-560.

[Comm12] Commtouch: Internet threats trend report (2012).

[DiKe11] D. Dittrich, E. Kenneally: The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, US Department of Homeland Security (2011).

[Inte07] Sophos facebook id probe shows 41% of users happy to reveal all to potential identity thieves. In: http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html, accessed 07-February-2013 (2007).

[JJJM07] T. N. Jagatic, N. A. Johnson, M. Jakobsson, F. Menczer: Social phishing. In: Communications of the ACM, ACM Vol. 50(10) (2007) 94-100.

[KiWM09] J. Kimmelman, C. Weijer, E. Meslin: Helsinki discords: Fda, ethics, and international drug trials. In: The Lancet, Elsevier Vol. 373(9657) (2009) 13-14.

[KKL+08] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, S. Savage: Spamalytics: An empirical analysis of spam marketing conversion. In: Proceedings of the 15th ACM conference on Computer and communications security, ACM (2008) 3-14.

[KKL+09] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, S. Savage: Spamalytics: an empirical analysis of spam marketing conversion. In: Communications of the ACM, ACM Vol. 52(9) (2009) 99-107.

[MBG+08] D. McCoy, K. Bauer, D. Grunwald, T. Kohno, D. Sicker: Shining light in dark places: Understanding the tor network. In: Privacy Enhancing Technologies, Springer (2008) 63-76.

[MPJ+12] D. McCoy, A. Pitsillidis, G. Jordan, N. Weaver, C. Kreibich, B. Krebs, G. Voelker, S. Savage, K. Levchenko: Pharmaleaks: Understanding the business of online pharmaceutical affiliate programs. In: Proceedings of the 21st USENIX conference on Security symposium, USENIX Association (2012) 1-16.

[SCC+09] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, G. Vigna: Your botnet is my botnet: Analysis of a botnet takeover. In: Proceedings of the 16th ACM conference on Computer and communications security, ACM (2009) 635-647.

[Thom84] K. Thompson: Reflections on trusting trust. In: Communications of the ACM, ACM Vol. 27(8) (1984) 761-763.

[TIS+98] J. A. Thomson, J. Itskovitz-Eldor, S. S. Shapiro, M. A. Waknitz, J. J. Swiergiel, V. S. Marshall, J. M. Jones: Embryonic stem cell lines derived from human blastocysts. In: *Science* Vol. 282(5391) (1998) 1145-1147.

[WHP+10] G. Wondracek, T. Holz, C. Platzer, E. Kirda, C. Kruegel: Is the internet for porn? an insight into the online adult industry. In: Proceedings (online) of the 9th Workshop on Economics of Information Security, ACM (2010) 1-14.