**Stellungnahme Referat Technik**

Aufgrund der aktuellen Entwicklung von sozialen Netzwerken hin zur Datensammelkrake sollte der StuRa diese Entwicklung nicht durch eigene Nutzung hinnehmen und die Probleme ignorieren, sondern die Studierenden für die datenschutzrechtlichen Probleme sensibilisieren.

**Änderungsantrag zum Beschluss:** Ablehnung der Nutzung von sozialen Netzwerken (insbesondere Facebook, Google+) und die Sensibilisierung von Studierenden zu datenschutzrechtlichen Problemen bei sozialen Netzwerken.
Dieser Antrag wird ebenfalls vom **Sozialreferat** (Referent Mike Niederstrasser), dem **Innenreferat** (Referent Sandra Schau) und dem **Vorstand** des Studierendenrates der FSU Jena unterstützt.

Als Vorschlag könnte man den AK InfoTech oder einen anderen AK wieder einrichten und dafür freiwillige MitarbeiterInnen suchen, die diese Aufklärungsarbeit leisten möchten.

Wir wissen dass soziale Netzwerke für den Kontakt zu Studierenden nützlich sein können, jedoch sollten wir den Nutzen nicht über die Gefahren stellen und diese einfach ignorieren.

Des weiteren möchten wir das Gremium darauf hinweisen, dass es auf das Fachwissen seiner ReferentInnen für die entsprechenden Themen zurückgreifen und selbiges auch beherzigen sollte. Als Entscheidungshilfe recherchierte das Referat Technik  und stellt einige Probleme dar.

**Vorbemerkung**

Bei der Recherche mussten wir mit Erschrecken feststellen, dass die Datenschutzprobleme umfangreicher sind als bisher angenommen. Leider kann hier nicht auf alles eingegangen werden und somit wurde sich auf das Soziale Netzwerk Facebook und auf die bedenklichsten Funktionen beschränkt. Dabei ist ein acht Seiten Bericht zustande gekommen.

# Bericht zu Risiken mit sozialen Netzwerken

## 1) Funktionen für die Datensammelleidenschaft von Facebook

### 1.1. Allgemeine Informationen

Einzelne und belanglose Informationen lassen sich verknüpfen und somit neue Erkenntnisse hervorbringen. Zum Beispiel hatte Mark Zuckerberg bekannt gegeben, dass er nichts mehr isst, was er selbst erlegt hat. In seiner „Timeline“ befindet sich ein Bild zu einem Bison. Zu einen späteren Zeitpunkt hat er ein Rezept für ein Gericht mit Bisonfleisch. Dies lässt die Schlussfolgerung zu, dass er ein Bison getötet und später gegessen hat. Solches lässt sich mit beliebigen Informationen machen. **Diese sind Einzeln zwar harmlos, sind aber verknüpft sehr aufschlussreich.**

### 1.2. Timeline

Aktuell führt Facebook eine neue Funktion namens „Timeline“ ein. Dies soll als eine Art Tagebuch fürs Leben genutzt werden. Daten können sowohl manuell in die „Timeline“ (zu jedem Zeitpunkt) eingetragen werden als auch automatisch durch „Apps“, die den Status des Nutzers sowie Handlungen in die „Timeline“ ohne Zutun des Nutzers hinzufügen können oder durch die „Open Graph API“ (Punkt 1.4), die es Webseiten ermöglicht die Tätigkeit des Nutzers auf der eigenen Website direkt in die „Timeline“ einzutragen . **Achtung!** Hierbei muss nur einmal in den Einstellungen zugestimmt werden. Dies ist vielen Nutzern zu einen späteren Zeitpunkt nicht mehr bewusst, andere lesen diesen Hinweis gar nicht erst und bestätigen Einfach um eine Funktion schnell nutzen zu können.

### 1.3. Like-Button

a) Allgmein

Der „Like-Button“ ist ein eine Schaltfläche, der auch auf Facebook-fremden Webseiten eingesetzt werden kann. Er bringt diverse Funktionen mit, die unter anderem Daten an Facebook übermitteln, wie auch Daten von Facebook an die Webseitenbetreiber. Er dient für den Nutzer dazu etwas als schön zu kennzeichnen und anderen Nutzern in Facebook mitzuteilen.
Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hat die Funktionen des „Like-Buttons“ analysiert und erklärt die technische Funktion und Wirkungsweise in einem Arbeitspapier.
Facebook setzt bei der Nutzung des Buttons ein großes Datencookie, welches mind. 2 Jahre Gültigkeit behält und somit immer wieder auslesbar ist.

b) Analyse der Nutzung von Webseiten auch bei nicht authentifizierten Nutzern

Facebook erhält generell bei jedem Aufruf einer Website, die den „Facebook-Like Button“ enthält, folgende Daten:

- Grunddaten, wie IP-Adresse und Browserstring
- Adresse der Webseite, eindeutige ID der Website
  *Anmerkung: Die ID hilft der besseren Zuordnung der Aktivitäten und vereinfacht die Verknüpfung und Verarbeitung von Daten.*
- Ablaufumgebung des Browsers, Bildschirmauflösung, Sprache, installierte Browser-Plugins

*Anmerkung: Dies erzeugt einen Fingerabdruck, der hilft den Nutzer auf anderen Webseiten auch ohne Cookie wieder zuerkennen. Dies ist ebenfalls ein großes Datenschutzproblem.*

Facebook erhält beim Betätigen des „Like-Buttons“ noch weitere Informationen:

- Daten mittels des zwei Jahre gültigen „datr“-Cookies

*Anmerkung: Das Cookie kann eine Sammlung weiterer Informationen enthalten.*

c) Nutzungsanalyse bei authentifizierten Nutzern

Ist ein Nutzer authentifiziert, z.b. durch eine aktive Session bei Facebook, dann führt Facebook bei Betätigung des Buttons weitere Javascripte die Funktionen zu Datenerhebung enthalten aus und legt weitere Cookies zur Informationsspeicherung und späteren Wiederabrufung/Wiedererkennung an.

d) Verstöße gegen das Gesetz

Der „Like-Button“ verstößt gegen die E-Privacy-Richtlinie § 15 Absatz 3 des Telemediengesetzes. Dies ist auch der Grund warum das ULD Schleswig-Holstein gegen den „Like-Button“ in der derzeitigen Form vorgeht.

### 1.4. Open Graph

a) Allgemein

Die Open Graph API ist eine Programmierschnittstelle, die es Anwendungsentwicklern oder anderen Webseiten ermöglicht Zugriff auf Daten direkt zu erhalten bzw. neue Informationen bei Nutzern zu ergänzen. Dies ist schon durch die initial von Facebook festgelegten Berechtigungen möglich. Für weitere Bereiche benötigt man nur eine Zustimmung durch den Nutzer aufgrund einer Anfrage nach weiteren Bereichen.

b) Funktionen und Möglichkeiten

Mithilfe der Schnittstelle sind eine Menge Funktionen möglich, die Daten von Nutzern auslesen und verarbeiten, sowie neue Daten hinzufügen können, die dann in der „Timeline“ ohne ein Zutun des Nutzers auftauchen. Diese Informationen mögen einzeln vielleicht noch kein Problem darstellen, aber in Verbindung mit anderen Informationen sowohl in der „Timeline“, als auch Informationen die andere Webseiten über ihre Nutzer kennen, sind komplette Interessen- , Nutzungs- und Bewegungsprofile möglich.
Durch die Erweiterungsmöglichkeit auf weitere Bereiche der Daten eine Nutzers durch eine Anfrage sind auch für externe Informationsverknüpfungen möglich um Profile zu erstellen oder weitere Erkenntnisse zu erlangen. Dies ist den Nutzern beim Bestätigen einer solchen Anfrage nie bewusst, da er darüber nicht aufgeklärt wird und die Funktionen für den Nutzer intransparent sind.

### 1.5. Facebook Insights

„Facebook Insights“ stellt detaillierte Statistikinformationen über Nutzer und Nutzerinnen zur Verfügung. Diese können von:

- Administratoren von Fanseiten,
- Anwendungsentwickler für die Facebook-Plattform,

- Webseitenbetreiber, die den „Like-Button“ verwenden,

genutzt werden.
Die Statistiken erlauben Rückschlüsse auf die Nutzung der Angebote. Dies sind unter anderem Nutzerzuwachsinformationen, Demographie, Nutzung von Inhalten, sowie das Erstellen von Inhalten (siehe FAQ von Facebook).
Auf diese Möglichkeiten hat der Nutzer keinen Einfluss, was dem Recht auf informationelle Selbstbestimmung widerspricht.
Des weiteren verstößt diese Funktion gegen das Trennungsverbot § 15 Absatz 3 Satz 3 des Telemediengesetzes der folgendes besagt „Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden“.

### 1.6. Gesichtserkennung

Im Juni 2011 führte Facebook eine automatische Gesichtserkennung ein. Mit dieser Funktion erkennt Facebook die Personen (die einmal ihr Profilbild erkennen lassen haben) in allen hoch geladenen Bildern und auch in Zukunft hoch geladenen Bildern, selbst wenn fremde diese Bilder hoch laden. Sollte eine Person erkannt worden sein, merkt sich das Facebook verknüpft dies mit den anderen Daten der Nutzer und bietet den Namen an und das Bild zu markieren. Selbst wenn man dieses Bild nicht markiert und somit öffentlich verknüpft, weiß Facebook dennoch von dieser Verbindung.
Ein kleines Beispiel. Sollte man zufällig auf einem Urlaubsfoto eines fremden Nutzer auftauchen, dann verknüpft Facebook alle Daten die mit dem Bild zusammenhängen, wie Orts-, Zeitdaten und Statusmeldungen, auch mit dem Nutzer der auf dem Bild erkannt wurde. Somit kann man erfahren wo und wann sich diese Person befand und ggf. welche Ereignisse zu diesem Zeitpunkt an diesem Ort stattfanden. Dies trägt ebenfalls zu Bewegungsprofilen bei.

## 2) Umgang mit den Daten

### 2.1. Verarbeitung und Analyse der Daten

Der Umgang mit den Daten von Facebook verteilt sich auf drei Ebenen:

- tiefste Ebene: riesige Datenpool indem unaufhörlich alle neuen Daten einfließen.
  *Anmerkung: Dies ist für den Nutzer intransparent, noch kann er kein Einfluss darauf nehmen.*
- Zweite Ebene: Hier werden die Daten durch unbekannte Funktionen veredelt, indem damit Verknüpfungen erstellt, Beziehungen der Subjekte gebildet, geclustert und Interessenanlagen der Mitglieder auswertet.
  *Anmerkung: Dies ist für den Nutzer intransparent, noch kann er kein Einfluss darauf nehmen.*
- Dritte Ebene: Hier läuft die Kommunikation zwischen den Nutzern. Erst hier gewährt Facebook ein paar Eingriffsmöglichkeiten in Form von Privatsphäre-Optionen.
  *Hinweis: Der Nutzer darf zwar Informationen gegenüber anderen Nutzern, aber nicht gegenüber Facebook unterdrücken.*

### 2.2. Weitergabe der Daten

Aufgrund der Enormen Sammlung von Informationen über Millionen Menschen (derzeit über 35 Millionen in Deutschland) steigt das Interesse diverser Gruppen an diesen Daten. Vor allem Facebook finanziert sich über Werbung und kann mithilfe dieser Daten, den Werbepartner eine gezieltere Werbung bieten und somit mehr Geld abknöpfen und

verdienen. Andere Firmen wollen auch was von diesem Kuchen abbekommen und interessieren sich daher ebenfalls für diese Daten. Facebook bietet ihnen über diverse Möglichkeiten auch Zugang zu einen Teil der Daten, wie zum Beispiel mittels „Like-button“, der Open Graph API sowie „Facebooks Insights“, welches schon bereits aufbereitete Daten zur Verfügung stellt.
Ebenfalls könnte Facebook auch erstellte Profile an andere Firmen verkaufen um den Gewinn zu steigern. Derzeit bestreiten Sie dies zwar, aber es kann sich dennoch jederzeit ändern.
Ein Anderes Problem ist, das die meisten Server von Facebook in den USA stehen und somit auch deren Gesetze Unterworfen sind. Dies bedeutet das unter anderem die USA selber Datenauskünfte verlangen kann. Das könnte z.b. Studenten betreffen die ein Auslandssemester in den USA absolvieren wollen und durch gewisse im Netz verfügbare Informationen die verknüpft wurden Aufmerksamkeit bei den Behörden auslösen, selbst wenn die Informationen nicht korrekt sind.
Nach Europäischen Recht steht auch jedem Nutzer die Möglichkeit offen, seine Daten die Facebook von sich speichert anzufordern. Dies hat ein Student gemacht und erhielt **1200** DIN-A4 Seiten mit Daten der letzten 3 Jahre, die auch gelöschte Informationen beinhalteten. Trotzdem musste er dabei feststellen das nicht alle Daten mitgeteilt wurden. Auf Nachfrage vom Focus erklärte Facebook laut Gutjahr, diese Informationen könnten nicht herausgegeben werden, es handele sich dabei um „Betriebsgeheimnisse oder geistiges Eigentum“.

## 3) Die größten Probleme

### 3.1. Privatsphäre-Einstellungen

Die Privatsphäre-Einstellungen hegen den Verdacht, dass Facebook mittels verkomplizierten Einstellungen die Nutzer dazu zu bringen mehr Daten zu veröffentlichen.
Ein Beispiel: Im Unterpunkt „Funktionsweise von Markierungen“ finden sich fünf Optionen, von denen bei nur vier Optionen die datenschutzfreundlichste Einstellung „Aus“ ist. Bei der fünften Einstellung, nämlich den Schalter für die Frage nach den manuellen Genehmigungen für jede Markierung auf fremden Beiträgen oder Fotos, bedeutet „Aus“ eine Verschlechterung des Datenschutzes. Dies bedeutet jeder darf den Nutzer ohne Nachfrage markieren und ihn somit mit weiteren Informationen verknüpfen. Dies dürfte Probleme beim Recht auf informationelle Selbstbestimmungen bedeuten.
Interessant ist, das selbst wenn die Einstellung eine Nachfrage fordert, weiß Facebook von der Verbindung schon vor der Zustimmung oder Ablehnung, sowie auch noch nach einer Ablehnung.

Mit jeder Änderung der Privatsphäre-Einstellungen und mit jeder Funktionserweiterung verlieren die Nutzer immer mehr die Herrschaft über ihre Daten.

### 3.2. Möglichkeiten der Datensammelleidenschaft

Die Möglichkeiten sind unbegrenzt. Mit den gesammelten Daten durch die unter Punkt 1) erläuterten Funktionen sind komplette „Lebensprofile“ möglich. Dies zeigt vor allem der Zweck der neusten Funktion „Timeline“, die ein Teil dieser Informationen als „Lebensblog“ darstellen möchte.
Es können derzeit Orts- und Bewegungsprofile erstellt werden. Durch die Open Graph API können dann komplette Kaufprofile (Interesse an Produkten als auch den Kauf von

Produkten), Interessensprofile (Welche Musik höre ich online, Welche Bilder schaue ich mir an, Welche Interessen/Hobbies habe ich, etc.).
Durch den Facebook-Like-Button sind ebenfalls Profile möglich die sowohl das Interesse als auch Geschmack eines Users erfassen.
Mithilfe der Gesichtserkennung können Nutzer Veranstaltungen, Orten zugeordnet werden, wo sie vielleicht nur zufällig vorbei kamen oder sich anonymisiert aufhalten wollen. Hierbei ist insbesondere das Recht auf anonyme Beteiligung an einer Demonstration zu beachten. Dies würde die Gesichtserkennung ignorieren. Somit könnte die Polizei mittels sozialer Netzwerke die Teilnehmer eine Demonstration erfassen und registrieren.
Dies sind nur ein paar Möglichkeiten. Grenzen sind hierbei nicht gesetzt.

### 3.3. Rechtliche Probleme

a) TMG § 15 Absatz 3 - E-Privacy-Richtlinie

Die aktuelle Version des „Like-Button“ verstößt gegen das TeleMedienGesetz §15 Abs. 3.

b) TMG §15 Absatz 3 Satz 3 – Trennungsverbot

Die Funktion Facebook „Insights“ verstößt gegen das Trennungsverbot des TeleMedienGesetzes.

c) Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung ist im bundesdeutschen Recht das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Es handelt sich dabei nach der Rechtsprechung des Bundesverfassungsgericht um ein Datenschutz-Grundrecht.
Hier verstoßen unter anderem folgende Funktionen

- Möglichkeit Adressbücher mit Daten dritter Personen hochzuladen (selbst wenn diese nicht bei Facebook angemeldet sind)
- Fotos mit Abbildungen Personen Dritter mit der Kombination der automatischen Gesichtserkennung (der man nur! einmal und nicht jedes mal zustimmen muss)
- Dauerhafte Speicherung von Daten auch nach Löschung der Daten durch den Nutzer, so wie der Verwendung für eigene Zwecke von Facebook.

d) Konsumenten- und Datenschutzrecht der EU

Facebook hat seine Nutzungsbedingungen weiter ausschließlich nach amerikanischem Konsumenten- und Datenschutzrecht gestaltet. Diese stimmen nicht mit den Konsumenten- und Datenschutzrechten der EU überein.

e) Weitere Probleme

Weitere Probleme sehe ich darin, das aufgrund der hohen Verfügbarkeit, die Daten nicht nur auf Servern in den europäischen Ländern gespeichert werden, sondern auch auf Server in den USA. Hier kann die USA nach ihren Gesetzen Daten einfordern um auch Informationen über Studierende die in die USA einreisen einzuholen. Dies kann schon bei verdächtigen Studiengängen der Fall sein. Das bedeutet das die Daten gegen die Regelungen der EU auch den Gesetzen der USA unterliegen.

Facebook schreibt in seinen Nutzungsbedingungen, dass es nicht sicherstellen kann, dass Daten sicher sind.

f) Aktuelle Anzeigen gegen Facebook

| Datum | Thema / Problem |
|---|---|
| 18-AUG-2011 | **Pokes (Anstupsen).**<br>Die Daten werden nach dem "entfernen" von Facebook weiter gespeichert und nie wieder gelöscht. |
| 18-AUG-2011 | **Schattenprofile.**<br>Facebook sammelt Daten von Personen im Hintergrund ohne, dass der Betroffene dies bemerkt oder dem zustimmt. Betrifft vor allem Personen ohne Facebook. |
| 18-AUG-2011 | **Markieren.**<br>Markierungen werden ohne Zustimmung des Users (Opt-In) aktiviert. Der User muss die Daten dann "entfernen" (Opt-Out). |
| 18-AUG-2011 | **Synchronisieren.**<br>Facebook 'saugt' persönliche Daten z.B. mittels iPhone-App oder E-Mail-Import ab und verwendet diese Daten für seine eigenen Zwecke ohne der Zustimmung des Betroffenen. |
| 18-AUG-2011 | **Gelöschte Postings.**<br>Posting auf den Seiten der Facebook Nutzern werden auch nach dem "entfernen" weiter gespeichert. |
| 18-AUG-2011 | **Postings auf fremden Seiten.**<br>Der User kann nicht herausfinden, wer die Daten auf fremden Seiten sehen kann. |
| 18-AUG-2011 | **Messages.**<br>Nachrichten (inkl. Chat-Nachrichten) werden auch nach dem "löschen" weiter gespeichert. Damit wird die gesamte direkte Kommunikation auf Facebook dauerhaft unlöschbar. |
| 18-AUG-2011 | **Datenschutzbestimmungen und Zustimmung.**<br>Die Datenschutzbestimmungen sind vage, unklar und widersprüchlich. Nach europäischen Standards ist die Zustimmung ungültig. |
| 18-AUG-2011 | **Gesichtserkennung.**<br>Die neue Gesichtserkennung ist ein unverhältnis- mäßiger Eingriff in die Privatsphäre der Nutzer. Außerdem fehlen Hinweise und die Zustimmung. |
| 18-AUG-2011 | **Auskunft mangelhaft.**<br>Die Auskunft, zu welcher Facebook gesetzlich verpflichtet ist, ist in vielen Punkten mangelhaft.<br>Viele Daten und Informationen fehlen. |
| 18-AUG-2011 | **Löschen von Markierungen.**<br>Markierungen (z.B. in Fotos) welche "entfernt" werden, werden von Facebook nur deaktiviert. |
| 18-AUG-2011 | **Datensicherheit.**<br>Facebook sagt in seinen Nutzungsbedingungen, dass es nicht sicherstellen kann, dass Daten sicher sind. |
| 18-AUG-2011 | **Anwendungen.**<br>Anwendungen von Freunden können auf die Daten des Nutzers |

| | |
|---|---|
| | zugreifen. Es gibt keine entsprechenden Sicherheiten, dass die Anwendungen europäischen Datenschutzstandards entsprechend. |
| 18-AUG-2011 | **Gelöschte Freunde.**<br><br>Freunde welche gelöscht werden, bleiben weiter auf Facebook gespeichert. |
| 18-AUG-2011 | **Exzessive Datennutzung.**<br>Facebook sammelt unglaubliche Datenmengen als "Host", die eigene Nutzung ist unlimitiert. |
| 18-AUG-2011 | **Opt-Out.**<br>Die Verwendung der Daten auf Facebook sind faktisch "Opt-Out" statt "Opt-In", das widerspricht den europäischen Gesetzen. |
| 19-SEPT-2011 | **Like** Button.<br>Der von Facebook derzeit angebotene "Like Button" ist nicht datenschutzkonform und kann zum ausspionieren der Nutzer verwendet werden. |
| 19-SEPT-2011 | **Pflichten als Auftragsverarbeiter.**<br>Facebook hat gegenüber den Nutzern die Pflicht die von Nutzer auf Facebook hinerlegen Daten nicht für eigene Zwecke zu missbrauchen. |
| 19-SEPT-2011 | **Privatsphäreeinstellungen bei Bildern.**<br>Die User können nur steuern wer den Link zu einem Bild sehen kann. Das Bild selbst ist für jeden abrufbar, der den Link kennt. Es gibt keine wirkliche Steuerung über Zugriffsrechte. |
| 19-SEPT-2011 | **Gelöschte Bilder.**<br>Gelöschte Bilder sind weiter abrufbar und werden erst mit großer Verzögerung gelöscht. Nur de Link zum Bild auf facebook.com wird unsichtbar. |
| 19-SEPT-2011 | **Gruppenmitglieschaft.**<br>Nutzer können ohne deren Zustimmung zu Gruppen hinzugefügt werden und müssen dann aktiv wieder austreten. |
| 19-SEPT-2011 | **Änderung der Datenschutzrichtlinien.**<br>Datenschutzbestimmungen werden regelmäßig, ohne entsprechender Information und ohne Zustimmung der User geändert. |

g) Weitere Informationen zu diesen Anzeigen könnt ihr auf der Webseite von www.europe-v-facebook.org nachlesen. Diese Seite ist unter den Quellen verlinkt.

### 3.4. Bedeutung für den Studierendenrat und die Studierendenschaft

Der StuRa setzt sich unter anderem für Menschenrechte und Rechte der Studierenden ein. Facebook missachtet jedoch einige europäische und deutsche (Grund-)Rechte. Durch die Teilnahme am Netzwerk würden wir jedenfalls nicht signalisieren, dass uns das ignorieren von Rechten durch Facebook stört.

Bei von uns propagierten Veranstaltungen, wie Demonstrationen fördern wir unter anderem die Verknüpfung weitere Daten. In diesem Fall ist es besonders kritisch, wenn Personen die per „Like-Button" gut finden, werden die Beziehungen gespeichert. Dies könnte z.B. der Polizei zur Recherche dienen um Teilnehmer von Demonstrationen zu ermitteln.

Laut den AGB würde Facebook die kompletten Nutzungsrechte für Bilder die der

Studierendenrat hochlädt erhalten. Hier ist auch zu beachten, dass nach löschen die Daten immer noch bei Facebook existieren. Ebenfalls muss beachtet werden, dass wir keine fremden Bilder verwenden dürfen, wenn wir nicht die kompletten Rechte daran haben. Das heißt, wenn wir nur „Nutzungsrechte“ haben, heißt es nicht, das wir andere auch zur Nutzung dieser berechtigen können, was aber Facebook in seinen AGB voraussetzt

Des weiteren tragen wir zu den sogenannten „Schattenprofilen“ bei, wenn Personen mit uns befreundet sind oder unsere Fan-Seite besuchen und auch mögen („Like-Button“).

Da gelöschte Postings bleiben erhalten bleiben, hat der Studierendenrat kein Einfluss auf die versehentlich geposteten Beiträge oder veröffentlichten Informationen.

Beratungen über Facebooks Messenger dürften keinesfalls durchgeführt werden, da diese Daten unlöschbar gespeichert werden, aber Beratungen nicht Dritten mitgeteilt werden sollten/dürften.

### 3.5. Gesellschaftliche Probleme

Auch wenn viele Nutzer wegen der aktuellen Datenschutzprobleme Bedenken hegen, überwiegt der Spaß an den Funktionen und der Nutzung immer noch diese Bedenken. Ebenfalls ist die Mehrheit der Nutzer sich nicht im klaren, welche Daten sowohl Facebook als auch Partner erhält und zu welchen Zeitpunkt der Nutzer zum Sammeln dieser Daten beiträgt, z.b. durch Besuchen von Webseiten der Partner oder mit dem Facebook „Like-Button“. Statt dessen ist **dringend Aufklärungsarbeit zu leisten**.

## 4) Fazit

Nach Recherche des Referat Technik ist ein eindeutiges Fazit zu ziehen. Es sollte keinesfalls eine solche Firmenpolitik, die Rechte von Menschen verletzt durch eine Nutzung, die zudem dann noch öffentlich propagiert wird, unterstützt werden. Wir sollten eher das Gegenteil unternehmen und die Studierenden über die Probleme aufklären. Die meisten Probleme sind den Personen entweder nicht bekannt oder die Auswirkungen nicht bewusst. Genau hier sollte der Studierendenrat ansetzen und diese Wissenslücke schließen.

## 5) Quellen / weitereführende Informationen


- Arbeitspapier des ULD Schleswig-Holstein https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf
- Report Facebook vs. Google: Datenschutz aus der c't 22/11 Seite 98ff vom 10.10.2011
- Report Facebook vs. Google: Funktionen aus der c't 22/11 Seite 92ff vom 10.10.2011
- http://www.test.de/themen/computer-telefon/meldung/Soziale-Netzwerke-und-Datenschutz-Was-Facebook-alles-erfaehrt-4271957-4271979/
- http://www.focus.de/digital/internet/facebook/datenschutz-beim-online-netzwerk-mitgliederdaten-geistiges-eigentum-von-facebook_aid_670053.html
- http://www.heise.de/newsticker/meldung/Facebook-Ein-Datenschutz-Hoax-und-eine-echte-Luecke-1350605.html
- http://www.spiegel.de/netzwelt/netzpolitik/0,1518,785177,00.html
- Anzeigen gegen Facebook: http://www.europe-v-facebook.org/DE/Anzeigen/anzeigen.html
- Facebook-FAQ
- wikipedia: http://de.wikipedia.org/wiki/Informationelle_Selbstbestimmung