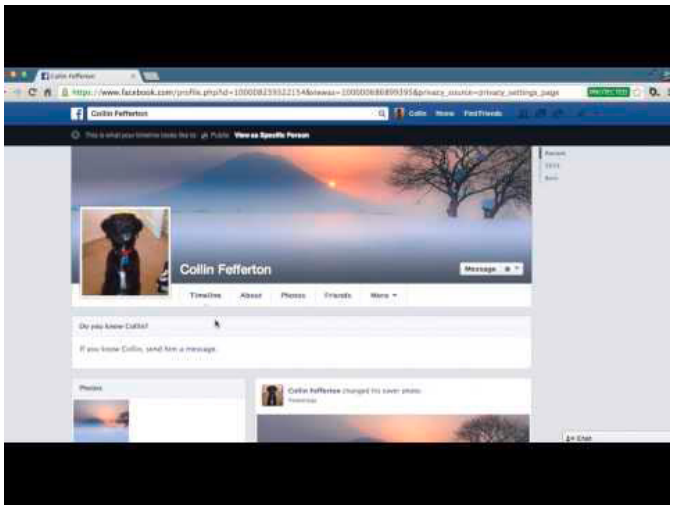
Kapitel 4: Ethische, soziale und politische Fragen

Video-Case 2: Datenschutz bei Facebook

Zusammenfassung

Das Geschäftsmodell von Facebook besteht darin, so viel private Daten über seine Nutzer zusammenzutragen, wie technisch möglich und gesellschaftlich vertretbar ist, und diese Informationen dann an Werbetreibende zu verkaufen, und zwar in Form von zielgerichteter Werbung auf der Website, der mobilen Site und den mobilen Apps von Facebook und auf den Websites der Facebook-Partner, die diese Informationen nutzen, um ihre Werbung zu personalisieren. Das folgende Video zeigt, wie Nutzer eine größere Kontrolle über ihre privaten Daten erhalten, die sie auf ihren Facebook-Seiten veröffentlicht haben.



https://www.youtube.com/watch?v=EjojvQLT7-c ; L=4:32

Video Case

In einem Interview von 2010 verkündete Mark Zuckerberg, der Gründer von Facebook, dass das „Zeitalter der Privatsphäre“ sich dem Ende zuneige. Laut Zuckerberg hätten sich die gesellschaftlichen Werte und Normen geändert und die Menschen hätten keine Bedenken mehr, ihre persönlichen Daten mit Freunden, Freunden von Freunden, ja sogar dem ganzen Web zu teilen. Diese Ansicht steht in Einklang mit Facebooks breiterem Ziel, die Welt zu einem offeneren und stärker vernetzten Ort zu machen (Zitat Zuckerberg). Viele Facebook-Funktionen basieren auf dieser Einstellung. Befürworter von Zuckerbergs Standpunkt sind der Meinung, dass das 21. Jahrhundert ein Zeitalter des „Informationsexhibitionismus“ ist, eine neue Ära der Offenheit und Transparenz.

Facebook hat eine lange Geschichte, die Privatsphäre seiner Nutzer zu verletzen. Genau genommen ist es die Grundlage von Facebooks Geschäftsmodell, die persönlichen Daten seiner Nutzer an Werbetreibende zu verkaufen. Im Wesentlichen funktioniert Facebook wie jeder andere Rundfunk- oder Kabelfernsehsender, der mit Unterhaltung versucht, große Zuhörer- oder Zuschauermengen zu erreichen und dann Werbetreibenden Sendezeit von 30–60 Sekunden für Werbeblöcke zu verkaufen. Natürlich können Fernsehsender mit den persönlichen Daten ihrer Zuschauer wenig anfangen und stellen somit eine viel geringere Bedrohung

der Privatsphäre dar. Facebook mit seinen 1,3 Milliarden Nutzern weltweit hat eindeutig ein großes Publikum.

Facebook, das in Harvard und anderen Universitäten seinen Anfang nahm, legte zu Beginn einfache Datenschutzrichtlinien zugrunde, der zufolge nur Freunde Zugriff auf Ihr Profil hatten. Dies änderte sich jedoch rasch, als Facebook-Gründer Mark Zuckerberg das große Ertragspotenzial einer öffentlich zugänglichen sozialen Netzwerk-Site erkannte.

2007 führte Facebook das Beacon-Programm ein, das dafür ausgelegt war, die Aktivitäten der Nutzer auf teilnehmenden Websites an deren Freunde zu senden. Sammelklagen waren die Folge. Facebook versuchte am Anfang, seine Mitglieder zu besänftigen, indem es die Funktion als Opt-in anbot, aber diese Maßnahme erwies sich schnell als Augenwischerei, da die persönlichen Daten auch weiterhin von Facebook zu verschiedenen Websites floss. Facebook stellte schließlich das Beacon-Programm 2009 ein und bezahlte 9,5 Mio. US-Dollar, um die Sammelklagen beizulegen.

2009 entschied Facebook einseitig, unbeeindruckt von dem Beacon-Fiasko, die persönlichen Basisdaten der Nutzer im Internet öffentlich zu machen, und verkündete, dass alle Inhalte, die die Nutzer bei Facebook eingegeben hatten, Facebook gehörten, und zwar für immer. Doch wie schon beim Beacon-Programm mündeten Facebooks Bemühungen, dauerhaft Kontrolle über die Nutzerdaten zu erhalten, darin, dass sich die Nutzer im Internet Widerstandsgruppen anschlossen und Facebook am Ende gezwungen war, diese Richtlinie ebenfalls zurückzuziehen. Die Nutzerunzufriedenheit auf breiter Front veranlasste Facebook, neue Grundsätze und eine neue Erklärung der Rechte und Pflichten vorzuschlagen, die von 75 Prozent seiner an der Online-Umfrage teilnehmenden Mitglieder angenommen wurde.

Die neue Richtlinie legte explizit fest, dass die Nutzer „ihre Daten besitzen und kontrollieren". Facebook verbesserte darüber hinaus seine Kontolöschfunktionen, beschränkte die Unterlizenzen zur Nutzung der Nutzerdaten und reduzierte den Datenaustausch mit externen Entwicklern. Dank dieser Maßnahmen kehrte für eine Zeit lang Ruhe ein. Doch leider waren seine resultierenden Datenschutzrichtlinien so kompliziert, dass die Nutzer in der Regel „Teilen" wählten, anstatt sich durch die über 170 Datenkategorien zu quälen, für die die Nutzer festlegen konnten, ob und für wen sie diese öffentlich oder privat halten wollten.

2009 führte Facebook außerdem seinen „Gefällt mir"-Knopf (Like) ein, der ab 2010 auch auf den Websites Dritter erscheinen durfte, um Facebook-Nutzer auf die angesteuerten Seiten und Käufe ihrer Freunde aufmerksam zu machen. 2011 begann Facebook, die Likes seiner Nutzer bei bestimmten beworbenen Produkten in den Sponsored Stories zu veröffentlichen (d.h. Werbung), einschließlich der Namen und der Profilbilder der Nutzer, ohne deren vorherige Zustimmung einzuholen, ohne sie zu bezahlen und ohne ihnen die Möglichkeit zu geben, auszusteigen. Folge war eine weitere Sammelklage, die Facebook im Juni 2012 für 20 Mio. US-Dollar beilegte. Im Rahmen der Beilegung erklärte sich Facebook bereit, seine Nutzer darüber zu informieren, dass ihre Daten wie Name und Profilbilder in den Sponsored Stories verwendet werden könnten. Außerdem wurde vereinbart, dass Nutzer und Eltern von minderjährigen Kindern eine größere Kontrolle darüber erhalten sollten, wie diese persönlichen Daten verwendet werden.

2011 veranlasste Facebook, dass alle seine Nutzer ein Gesichtserkennungsprogramm durchliefen, ohne diese vorher zu fragen. Wenn ein Nutzer Fotos hochlädt, erkennt die Software die Gesichter darauf, versieht sie mit einem Tag und erzeugt einen Datensatz von dieser Person/Foto. Später können Nutzer alle Fotos anzeigen lassen, auf denen ein bestimmter Freund abgebildet ist. Jeder vorhandene Freund kann mit einem Tag versehen werden und die Software

schlägt die Namen der Freunde als Tag vor, wenn Sie die Fotos hochladen. Auch dies rief die Datenschützer auf den Plan, die Facebook zwangen, den Ausstieg aus dieser Funktion für die Nutzer leichter zu machen. Aber die Bedenken bleiben.

Im Mai 2012 ging Facebook an die Börse. Dadurch stieg der Druck, Umsatz und Profit zu steigern, um den Aktienkurs zu rechtfertigen. Kurz danach kündigte Facebook die Einführung eines neuen mobilen Werbe-Features an, das ohne Erlaubnis der Nutzer Anzeigen auf deren mobile Newsfeeds hochlädt, und zwar auf Basis der Apps, die sie über die Facebook-Funktion Connect verwenden. Facebook soll angeblich sogar die Möglichkeit haben, zu verfolgen, was die Nutzer mit ihren Apps machen. Außerdem kündigte Facebook sein neues Feature Facebook Exchange an, das es Werbetreibenden ermöglicht, Anzeigen bei Facebook-Nutzern auf der Basis ihres Browserverhaltens außerhalb des Facebook-Systems zu schalten.

2011 wurde Facebook von der Federal Trade Commission verklagt, die Facebook zur Last legte, dass es seine Nutzer in der Zeit von 2009 bis 2011 hinsichtlich des Teilens von Daten mit Werbetreibenden systematisch betrogen hatte. Im Dezember 2012 legte Facebook diesen Streit mit der FTC endgültig bei. Das Unternehmen musste versprechen, dass es seine Nutzer „klar und deutlich“ darüber informiert und deren Einverständnis einholt, wenn es deren Nutzerdaten außerhalb der Privatsphäre-Einstellungen teilt. Außerdem muss sich Facebook zweimal jährlich für die nächsten 20 Jahre einer Datenschutzprüfung unterziehen und ein „umfassendes Datenschutzprogramm“ einführen.

2011 wurde gegen Facebook eine Sammelklage von Nutzern eingereicht, die ihre Privatsphäre ab dem Zeitpunkt verletzt sahen, als Facebook ihre Bilder in den Sponsored-Story-Anzeigen ohne ihre explizite Genehmigung zeigte. Im Dezember 2012 legte Facebook eine 20 Mio. US-Dollar Sammelklage bei, die von Nutzern eingereicht wurde, die Anstoß an der Sponsored-Story-Werbung von Facebook nahmen.

2013 und 2014 standen weitere Facebook-Aktionen im Kreuzfeuer der Datenschützer. Eine CNBC-Umfrage ergab sogar, dass Facebook das Technologieunternehmen ist, dem die Nutzer hinsichtlich des Datenschutzes am meisten misstrauen.

Wenn Sie weiterhin vorhaben, Facebook zu nutzen, und dabei zumindest einen Teil Ihrer Privatsphäre schützen wollen, dann schauen Sie das Video, das beschreibt, welche Schritte Sie dazu ergreifen müssen.

Fragen zu dem Video-Case

1. Haben Personen, die Facebook nutzen, einen Rechtsanspruch auf Privatsphäre, wenn sie selbst Informationen über sich posten?
2. Wie können Änderungen an Ihren Connection-Einstellungen auf Facebook dazu beitragen, Ihre Privatsphäre zu schützen?
3. Wie können Sie verhindern, dass Ihre Zeitleiste von Google oder anderen Suchmaschinen indiziert wird?