Policy Recommendations for Improving the Current State of Terms of Service Contracts

Mehitabel Glenhaber

Hannah Wei

Jenny Yao

Executive Summary

The widespread and increasing use of “dark patterns” [1] and other techniques of subtly manipulating consumers into unintentional choices while purchasing products or agreeing to Terms of Service (ToS) contracts, violates commerce rules (of the Commerce clause of the U.S. Constitution) against deceptive marketing. We propose a remedy of industry-set, best-practice, guidelines under federal supervision, as well as the development of privacy monitoring software allowing consumers to track how third-party applications are actually using privacy-sensitive information. These two measures can establish enforceable industry standards without chilling innovation. These standards, moreover, can be aligned with both European OECD standards and US policies laid out by the FTC privacy notice proposal, the Consumer Privacy Bill of Rights, and FIPPS.

We specifically focus on the technological factors of UI (user interface) of current ToS contracts, and the ways that these design factors can be abused to influence user decisions. UI is focused on what the user sees; the design of a UI can also change the way that a user interacts with a service, including influencing their decisions regarding a ToS.

Abuses happen when companies employ dark patterns, or UIs specifically designed to trick users into making choices against their best interests. Dark patterns can influence users by obscuring information, presenting information misleadingly, or simply using subtle cues to bias users towards certain options. With a plethora of dark patterns emerging in the UIs of many ToS contracts that users see today, it becomes harder and harder to avoid getting tricked by unscrupulous companies and websites.

While current judicial precedents have deemed regular ToS as enforceable because they are usually both clearly presented and explicitly agreed to by users (*Schnabel v. Trilegiant Corp*), there is clearly a misalignment because the government does little to ensure that users are not being manipulated into agreeing by UIs [2]. In many cases, while courts considers the accessibility of the ToS itself, they do not consider the more subtle effects of deceptive UIs on user decision making. The OECD recommendations [3], FTC’s privacy notice proposal, Consumer Privacy Bill of Rights [4], and FIPPs, all stress the importance of users not only giving consent but giving *unbiased, fully informed* consent for their data to be used. The only

way to support the user's rights to privacy protection and transparency would be to bring regulations on ToS into alignment with these directives, namely by regulating UIs and dark patterns to ensure that a user giving consent means that they are giving *fully informed* consent.

The government, the users, and the companies are all major stakeholders in this issue. Of course, it would be exceedingly difficult to develop a proposal that would satisfy all the stakeholders in this issue. Our proposal seeks to find the best compromise between these parties by first raising awareness of the content and meaning of ToS contracts through software solutions and second, creating guidelines for interfaces that are more intuitive and clear to navigate without limiting companies too strictly. Specifically, we propose that the FTC assemble a set of guidelines for usability and transparency which companies must abide by in UIs related to contract with users, and that the government encourage the development of software solutions to counteract dark patterns and inform users about the choices that they are making. Our proposal will protect the users, but at the same time, we will not unfairly place a burden on companies or impinge on the ability of companies to innovate, so long as they are not employing any misleading UI designs. We will also make it more straightforward for the government to evaluate ToS contracts and decide whether or not they are constitutional or enforceable.

Contents

1 Background

In recent years, there has been a huge expansion of digital services that Americans use every day. As such, the meaning of making a legal agreement, especially with regards to what a company may do with one's data, has changed significantly. Any time someone downloads an app, creates an online account, or installs a software package, they almost always have to agree to a Terms of Service contract, sometimes unknowingly. Terms of Service agreements (ToS), or sometimes more specifically categorized as End User License Agreement (EULA) for certain software, are an essential part of the modern individual's life. Globally, an individual agrees to an average of 26 ToS contracts through their smartphone alone [6]. As mentioned earlier and reiterated in research done by Sundar, Auriemma and Waddell, most people do not read ToS carefully, as they are seen as "dull, dense and inaccessible" in terminology and presentation [7]. This is no surprise, as the reading level of many ToS's are often at a college reading level [8], while the average reading level of American adults is around 7th to 8th grade [9]. Additionally, the majority of ToS are several thousands of words long [8]; at an average adult reading pace of 250 words per minute, it could take up to 20 or 30 minutes to read. Additionally, confusing UIs, either designed poorly or intentionally designed to trick users, make it even more difficult for users to understand the already obscure terms they are agreeing to.

In this paper, we aim to address the current areas of ToS contracts that are in need of improvement. We offer a two-pronged proposal to not only regulate the design of ToS contracts, but also to encourage the development of software tools to aid users in understanding the ToS contracts that they are presented with, so that they can make a more informed decision on whether or not they will comply with said contract.

1.1 Summary of Policy Issues

The first issue that must be addressed is the UI, or user interface, of typical ToS contracts. Internet users must negotiate complicated relationships with companies concerning the use of their personal data, involving contracts that can vary service to service, and which it is often not in a service provider's best interests to clarify. In fact, many service providers make no attempts to clarify their ToS. Others use tactics to intentionally obfuscate terms of service, either through the wording of the ToS itself (for example, by making their ToS excessively long or full of jargon) or through the UI by employing deceptive UIs known as dark patterns. These unscrupulous actions are made possible by the fact that there is currently little regulation of UIs relating to ToS contracts (or for any other purpose) in the United States.

Dark patterns are a direct result of this freedom. Also called "Evil Interfaces", deceptive UI, and a variety of other names, dark patterns are UI designs which intentionally and malevolently "trick" users into making decisions against their best interests, while not actually presenting any false information. They have become increasingly popular in the past few years [1]. Many dark patterns are technologically advanced and subtle versions of age-old cons or scams, but are widely employed by many major internet service providers. Many of these tricks, such as "trick questions" or "hidden menus" have also been adapted to fit the the scope of ToS contracts, as will be discussed in section 3.

1.2 Analysis of the Values at Stake

The companies who utilize ToS contracts and the users who agree to these contracts are two important stakeholders within this issue. The US government, as the arbitrator between these two parties, is a stakeholder as well. The first core value that unites these stakeholders is that of trust. Just as the US government has a vested interest in making sure that citizens are not falling victims to scams or predatory contracts, it has an interest in protecting consumers from manipulative data collection contracts. Trust, in the form of transparency and making sure that users are aware of the choices they are making (especially regarding privacy), is one of the main points of the White House's Consumer Privacy Bill of Rights [10], and is an important value to consider in this issue. Similarly, in discussing informed consent, the OECD Privacy Guidelines note that “behavioural research has shown that how information is presented, or framed, can have dramatic effects on how consumers respond to that information” [3]; it recommends that policymakers consider the way that information is presented as well as what the information is. Following these two documents, we believe that when legally considering a user’s consent for a company to use their data, only fully informed consent given without the interference of manipulative UIs should be counted. Users should be able to trust that companies are not manipulating them, and should know that when they make a choice regarding their privacy they are making the choice they think they are making. Companies should not try to hide aspects of their ToS from users and should be making contracts with informed users, not keeping them in the dark and scamming them.

Another critical value that plays a role in this issue is that of privacy. Though privacy is not explicitly outlined in the Constitution, it is considered an important fundamental right (for example, the Fifth Amendment protects against self-incrimination, which in turn protects the privacy of personal information). In recent times, Internet users have been increasingly conscious of their electronic footprint. In fact, a 2016 Pew research poll found that 86% of Internet users have taken steps online to remove or mask their digital footprints, and another 61% would have liked to do even more [11]. A significant 91% of respondents believed that consumers have lost control of how personal information is collected and used by companies. It is clear that the use of deceptive practices by companies, which involve incursions upon the privacy of their customers, is considered an important issue by most Internet users, and that work needs to be done to assuage their concerns.

Users concerns about privacy should be taken seriously, because with increased data collection by digital services, privacy breaches can be very serious [12]. There is huge potential for abuse for data collected by companies without a user’s knowing consent. According to an FTC report, when users were informed of how much data companies were actually collecting on them, and what the data was being used for, they frequently viewed the companies’ practices as “underhanded.” [13] In a recent, high profile case, Facebook manipulated users newsfeeds without their knowing consent in order to study user’s emotional responses to seeing more positive or negative news stories, an experiment that had profound emotional effects on many users, and was viewed as an extreme breach of trust [14]. Unethical experiments without user consent are just one of many ways that companies can abuse user agreements to ToS which they do not fully understand. And even when a company itself does not abuse data it has collected without a user's fully informed consent, there is still the danger of security breaches, as any user data stored by a company is also in danger of being accessed by malevolent hackers. One specific case is Snapchat: the ephemeral-based multimedia-sharing platform marketed itself as a private and temporary communication platform in which all content would be removed after the intended use of Snapchatters. However, in late 2013, over 4.6 million phone numbers, usernames, and location data were leaked online and could easily be linked to specific Facebook or Twitter accounts [15]. This led to heightened review of Snapchat's ToS and privacy policy, both of which shocked most users. Had users fully understood Snapchat's privacy policy, they would have been able to make better decisions as to whether they trusted snapchat to keep their data safe. Although this massive incident led to Snapchat's reformed policies around data permissions and user protections, most app companies still fail to be scrutinized until they run into substantial privacy problems.

Lastly, we value innovation, because it is perhaps the greatest driving factor behind our ability to progress as a human race. According to a recent global PWC survey of 1,200 CEOs, "innovation, along with increasing their existing business, now outstrips all other means of potential expansion" [16]. While we wish to protect the privacy and rights of the people, we also do not want to stifle creativity and innovation by enacting unnecessarily restrictive policies upon the companies that provide essential products and technology to the world. Ideally, a balance could be reached between the innovative freedom of businesses and the protection of the user's privacy.

2 Human Computer Interactions and Dark Patterns

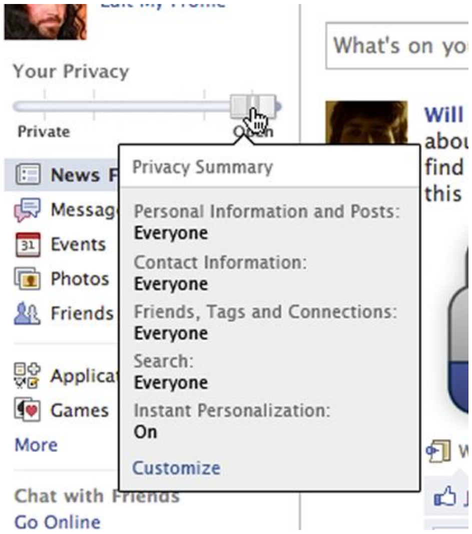
As mentioned previously, the primary factor influencing terms of service agreements is their UI design which, intentionally or unintentionally, bias users towards certain decisions. The term "dark patterns," frequently used in online privacy activist circles, (and catalogued at www.darkpatterns.org) refers to UI designs which do not actually present any false information, but whose purpose is to dupe their victims into giving away personal information, purchasing items they had no intention of buying, or a variety of other negative outcomes. Dark patterns employ tactics such as deceptively directing the user's attention, confusing the user about the meanings of their options and their choices, or making it difficult for users to find critical information. The study of Human Computer Interactions (or HCI) offers us valuable new insights into the ways designs influence users decisions, as well as ways to reform ToS-related UI in order to make users more informed and unbiased in making decisions regarding their online activity, including what information they allow companies to collect about their online activities and whether they allow companies to show them targeted ads.

Dark patterns often rely on three major devices in order to influence user behavior. The first one is lack of transparency, where an app does not make information about its actual functioning or terms of service readily available. Transparency is one aspect of UI design which has been regulated relatively thoroughly by the FTC and other organizations. The second device is obfuscation, where information is made difficult to find or read, for example by hiding it in a menu that makes it difficult to find, or using confusing phrasing or color coding to make it hard for users to make sense of information. The third device is deception, where a UI actually leads a user to believe false information, perhaps by conflating two similar settings. An app can be perfectly transparent (technically make all the information about privacy settings available to consumers) while also employing techniques of obfuscation and deception, rendering its transparency useless. In our proposals, we seek to address these issues of obfuscation and deception similarly to how the FTC has already addressed transparency

Of the attention which has been directed to dark patterns so far, much of it has focused on dark patterns designed to cheat consumers out of their money, but dark patterns are also employed in UIs related to ToS and privacy settings. There has been much attention directed to dark patterns such as "Forced Continuity," where a user is charged continuously for a pay-per-month service that is hard to cancel, or "Sneak Into Basket", where an item is added to a user's "cart" causing them to accidentally buy it without placing it there, are mainly used in commercial transactions, to simply extract more money from their victims [1]. However, other dark patterns are frequently used by websites and mobile applications to extract information from users which they would prefer not to disclose, or to get users to agree to privacy-related contracts which they do not realize they are agreeing to. In this paper, we examine several tactics frequently used to obfuscate privacy-related choices: hidden menus, and trick questions

2.1 Examples of Dark Patterns Used Specifically in ToS Contracts

Faceook's user interfaces surrounding privacy (partially shown below) are a good example of use of obfuscation and deception in privacy related UIs [17].



Privacy Summary

Personal Information and Posts: Everyone

Contact Information: Everyone

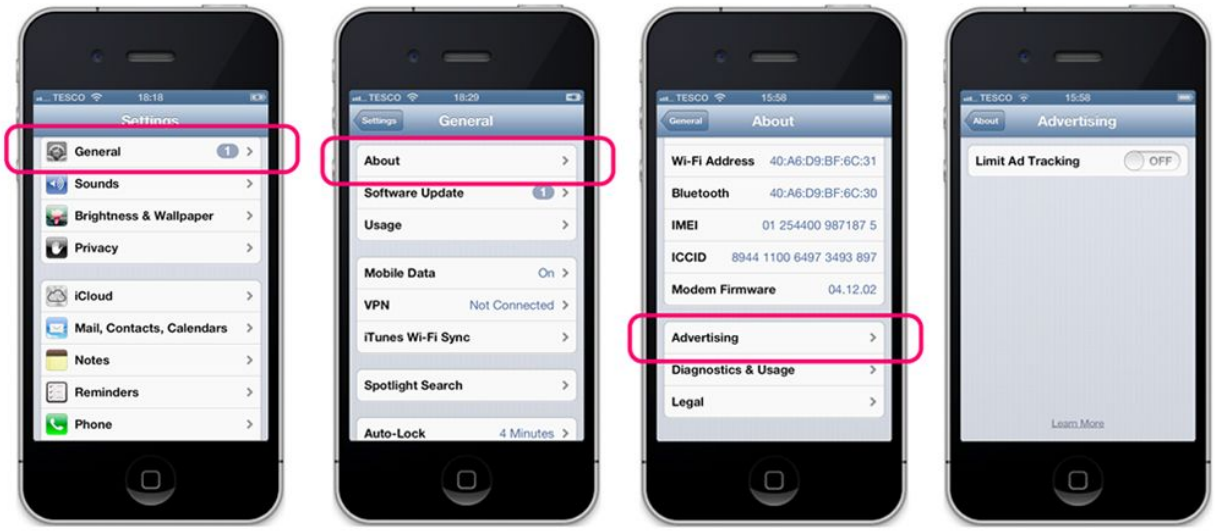
Friends, Tags and Connections: Everyone

Search: Everyone

Instant Personalization: On

Figure 1. Facebook's "privacy slider" which leads uses to believe they are changing how much information they share with Facebook, when they are actually changing how much information they share with other Facebook users. (Image via Wired.com)

Facebook's UI consistently uses confusing wording to encourage users to conflate information that is shown on their profile to other internet users and information which is displayed to Facebook itself. In their settings menu, users can adjust a "privacy slider", which they might easily believe controls what information about their activity Facebook may track, because it is the only obvious privacy setting and does not specify what sort of privacy it adjusts. However, this slider actually adjusts what other Facebook users can see about a user's activity, not what information on that user Facebook may collect. This is a clear case of deception, using ambiguous wording to suggest that a setting does one thing when in fact it does another. Furthermore, if a user were to go looking for the actual settings menu to adjust how much of their activity Facebook may track, they would have to search through a number of nested menus in order to find it. Additionally, Facebook procedures for adjusting privacy settings are very complicated, often requiring them to visit a series of different pages, or even visit the same page twice, and give users no warning when they have completed the steps partially but not fully. This is an example of obfuscation, making certain information or settings hard to find to discourage users from trying to find them. The simplicity and easiness of the "privacy slider" in contrast to the deep chain of menus a user must navigate in order to change the real privacy settings makes it clear that Facebook is attempting to encourage users adjusting certain settings, and discourage them from adjusting others. Many other major companies use this sort of tactic to some degree, as shown below. .



Mobile Data On

VPN Not Connected

Auto-Lock 4 Minutes

Wi-Fi Address 40:A6:D9:BF:6C:31

Bluetooth 40:A6:D9:BF:6C:30

IMEI 01 254400 987187 5

ICCID 8944 1100 6497 3493 897

Modem Firmware 04.12.02

Limit Ad Tracking OFF

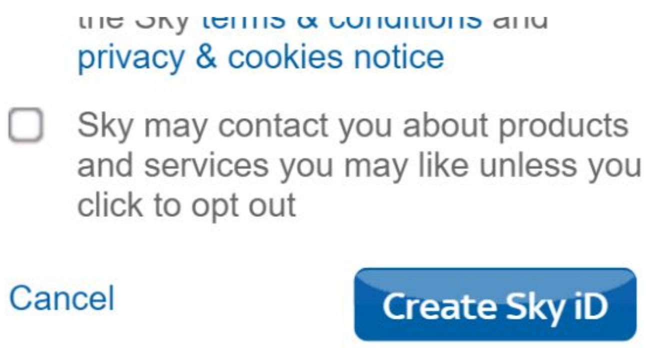
Figure 2. The complete sequence of menus which a user must sift through in order to change ad tracking settings for Apple iOS 6. (Image via SBnation)

Hidden Menus

Another dark pattern that is frequently used to obfuscate privacy settings is hard to find privacy settings hidden in menus. Rather than present users with obvious privacy options upon registering an account, many mobile apps and websites will instead begin with default settings and hide the options to change them deep in menus which users are unlikely to look through. Especially when combined with opt-out rather than opt-in privacy settings, hiding options in menus can coerce users into agreeing to contracts without their knowledge [18]. For instance, in iOS 6, Apple introduced ad tracking, and gave readers the option to opt-out and remove themselves. However, the option to opt-out was hidden in an “advertising” menu in a “about” menu in the “general” menu, rather than in the “privacy” menu with other privacy settings. The complete series of menus that a user must navigate in order to change the ad tracking setting is shown above. Users were not obviously made aware of an opt-out choice, and even if they had been, the choice would have been frustrating, perhaps impossible for some users, to find. Facebook and Google have also been observed using similar strategies and obfuscating privacy options from users. This is an instance of obfuscation, making it hard for users to adjust settings, as well as a failure of transparency in disclosing default settings and methods for changing them.

Trick Questions

The third sort of dark pattern which often appears in privacy related contexts are “trick questions”, which are worded to confuse the user into making a different choice from the one which they intended to make. Trick questions often involve the use of double negatives, or switching between negative and positive statements from one line to the next. For instance, in the example with the Apple ad-tracking menus mentioned above, when the user finally got to the opt out option the user is presented with an option to “limit ad tracking” (turned off) rather than an option to “allow ad tracking” (turned on), so that the user is likely to see “ad tracking” and “off” and assume, unless they have been reading carefully, that the ad tracking has been turned off [18].



the Sky terms & conditions and privacy & cookies notice

□ Sky may contact you about products and services you may like unless you click to opt out

Figure 3. A "trick question" dark pattern employed by Sky. The phrasing of the question leads the user to believe that checking the box will subscribe them to receiving spam emails, when in fact it will unsubscribe them. (Image via One2One IT)

Trick questions often use our associations with checked boxes or the phrase "on" as affirmative in order to create subtle double negatives or to confuse users as to if they are choosing to select or not to select a positive or negative option. Other sites create trick questions by wording their options in biased ways, stressing the benefits of continued data collection when users move to make choices to protect their privacy, such as messages from Facebook which refer to a data collecting service as "personalization," stressing the benefits to the user, and describing the benefits of "personalization" and the presumed difficulty of restoring the option once it is opted-out of [17]. Trick questions work by confusing the user and manipulating them into choices they might not intend, either through logically confusing them as to what their options are, or emotionally confusing them about the effects of their choices. Trick questions are a case of outright deception, sometimes combined with obfuscation, which trick users into making choices they would not otherwise make.

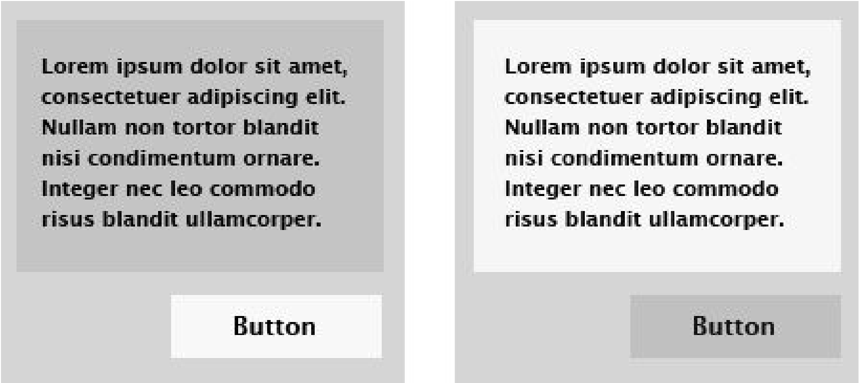
2.2 Current Research on Usability Guidelines

If a dark pattern is an intentionally confusing and obfuscated UI, which deceive and trick users, then the opposite of a dark pattern is a well designed, usable, non-deceptive UI that is simple for users to interact with. Not all dark patterns are even necessarily intentionally deceptive UIs. Many of them, such as some hidden menus or forced continuity UIs, may sometimes manifest as simply poorly designed UIs which are confusing and difficult for users to navigate. However, there are very few incentives for companies to design a good UI when a bad UI is making them money by tricking users. Thus, guidelines for better usability would eliminate many dark patterns which rely on obfuscation, whether they are intentional or not. Various experts in UI design have proposed sets of guidelines for usability and transparency, or rules for designing a UI which is straightforward, non-deceptive, and easy to use.[19] A set of guidelines outlined by usability.gov make similar recommendations and several others, including using color, typeface, and size to indicate hierarchies and make for easier reading, and using purposeful layouts to direct user attention, and maintanin consistency between pages, and even between different UIs that users may be familiar with [20]. Suzanne Martin outlines specific rules for using typesetting and color in UI design, including recommending a“maximum of 3 typefaces in a maximum of 3 point sizes...a maximum of 40-60 characters per line of text ...set[ting] text flush left and numbers flush right [and] avoid[ing] centered text in lists and short justified lines of text.”

However, simply preventing obfuscation is not enough to completely counteract dark patterns as some dark patterns are perfectly usable and non-obfuscated UIs which are nonetheless deceptive. Thus, we must expand our set of usability guidelines to include guidelines for transparency to prevent deception. For example, one researcher, Jakob Neilsen, outlines ten usability heuristics for UIs which tackle many issues of transparency. His recommendations include consistently using the same words for the same things, always giving users easy “undo” options, giving users feedback indicating the state of the system and changes they have made to it, minimalist design without distracting details, and good documentation

Suzanne Martin also recommends using several colors to group related items, following cultural associations with those colors (such as green as affirmative and red as negative) [21]. Usability Post recommends using light and darkness to direct the user’s attention to important elements.

Dark patterns are often violations of these principles, and by mandating the use of these principles, many dark patterns could be avoided. For example, Neilsen and Usability.gov’s recommendations for making user options clear and giving feedback are violated in Facebook’s privacy interface which makes user options very unclear, confusing them about whether they have changed their privacy settings by not giving them any sort of feedback. Requiring that users have easy “undo” options would counteract forced continuity dark patterns, which make it difficult for a user to take back a choice. Many trick questions could be avoided with requirements for straightforward stating of user options, or simply requiring consistency between checkboxes and green/red color coding making it clear if the user is agreeing to an affirmative or negative statement by ticking a box. Using clear typesetting with size, typeface, and color being used to indicate emphasis, when used to actually direct user attention to important details, could be an effective way to get users to pay attention to the terms and conditions they are agreeing to. For example, the figure below shows two possible designs for a popup window presenting a user with a ToS document and a button to agree to it. By highlighting the document rather than the button, UI designs could encourage users to read the text, rather than encouraging them to rush to clicking the button without reading the document. Since dark patterns rely on deceptive or confusing designs, they can be controlled and prevented through mandating good design principles.



Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Nullam non tortor blandit nisi condimentum ornare. Integer nec leo commodo risus blandit ullamcorper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Nullam non tortor blandit nisi condimentum ornare. Integer nec leo commodo risus blandit ullamcorper.

Figure 4. Two possible UI designs for a ToS popup window. The dark pattern design is shown on the left and the optimal design on the right. (Image via UsabilityPost)

Thus, based on this research we suggest a set of UI guidelines for usability and transparency designed to prevent obfuscation and deception. We suggest four main principles of usable and non-deceptive UI design: consistency, honest formatting and direction of attention, transparency and feedback, and finally, user control and undo options.

There is already a strong precedent for US regulatory bodies recommending or mandating good design principles, especially when it comes to protecting consumers from unfair business practices and requiring that certain information be disclosed. For example, good design principles, such as readability and consistency, are an important part of nutrition facts labels. In this particular case, the FDA requires that food manufacturers provide certain information which is used to fill out a strict template which has already been confirmed for readability. The success of the nutrition facts label is based in its consistency; consumers only need to learn how to read it once, and then have the necessary skills to determine the nutritional information of any food with a nutrition facts label. The FTC also usability and readability for information disclosures, though they do so through a less strict set of guidelines. In their recent report on mobile privacy disclosures, the FTC maintains the good design principles are an important part of privacy disclosures. They recommend using icons and quick facts sheets or "privacy dashboards" to make information easily and quickly available to readers, and suggest a requirement that privacy disclosure be typeset and spaced such that they are easy to read, and contain visual hierarchies to help users locate information [13]. The report also recommends greater consistency between privacy disclosures for apps, recommending some degree of standardization, or even a rigid template which would work as a sort of "privacy nutrition facts." We agree with these recommendations and believe that these guidelines, combined with usability guidelines for UIs, should be adopted for UIs dealing with ToS as well as privacy disclosures. Guidelines of this sort have been very effective in other areas, such as nutrition, and in this case would be effective at preventing dark patterns as well as increasing general user awareness of digital privacy.

2.3 Current Research on Software Solutions

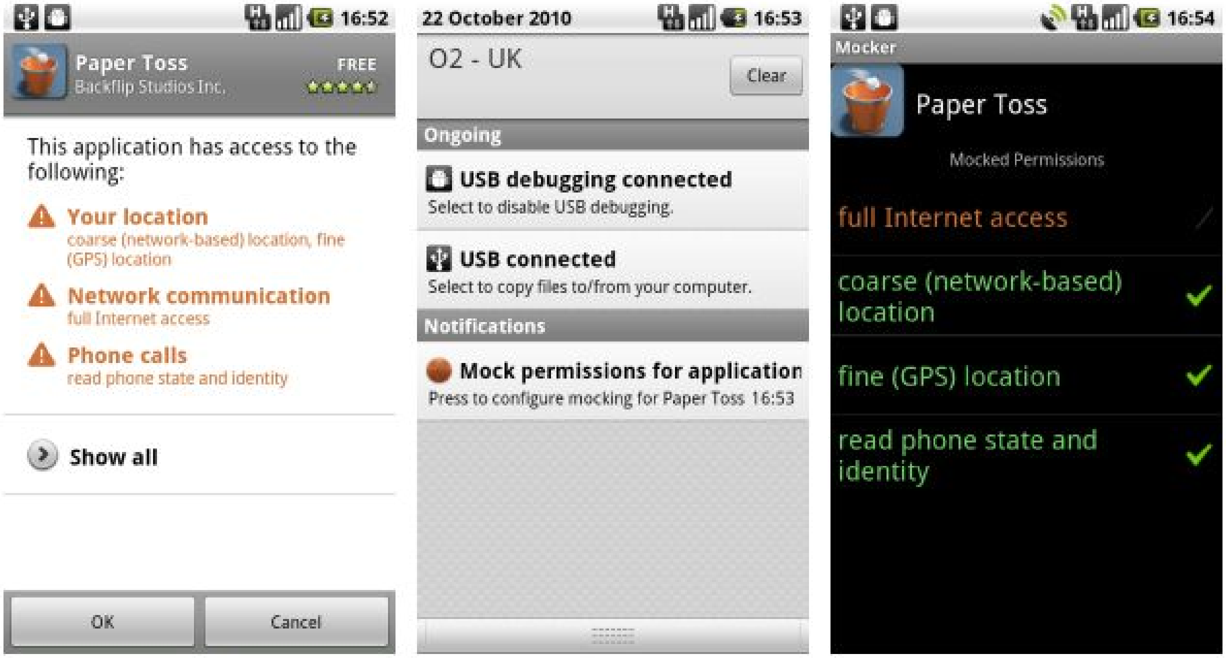
Our second proposed solution to the problem of dark patterns is the development of software solutions. Most of the following software technologies are at the forefront of HCI design, but they are difficult to be used by non-technical individuals because they require skills such as jailbreaking of mobile devices or altering of an app store's permission request interface. Because of these barriers, some critics would contend that these privacy-awareness tools are not real solutions to the problem, which is that most mobile application consumers are not knowledgeable or conscious enough of their mobile privacy—even if they are, they have acquired learned helplessness through past experiences of repeated invasion by internet services into their personal mobile privacy and have given up on finding options to protect their data [34]. While the critics are correct in that these software solutions have a high barrier to use by the regular mobile user, our recommendations are encouraging the government to work mainly with the application providers to implement these solutions, educate the average user, and provide these software solutions as simple options for the users to leverage without having to break their set behaviors. The software solutions devised by HCI specialists that can be feasibly implemented are TaintDroid, MockDroid, Recon, app store sensitivity scores, and Privacy Leaks. We will first introduce them and discuss current benefits and drawbacks of each. Later they will be combined into a Privacy Awareness Kit to be used as a basis for our recommendations.

The TaintDroid, developed by Penn State University and Duke University under the support of Intel Labs and the US National Science Foundation, allows for the real-time monitoring of how apps are managing a user's privacy-sensitive information by tracking the information leaving a user’s phone and providing a detailed breakdown on which pieces of personal data are being extracted, and where they are going. According to their studies, over half of the most popular applications share private user data with remote third-party advertisers. This private user data at risk is also known as personally identifiable information (PII), and include digitally mobile data such as geographic location, unique phone identifier, phone number, SIM number, usage history, microphone input, and camera images. More often times than not, the use of this sensitive information is not even clearly disclosed in the ToS.

Strengths of this software include efficiency and simple clarity. As mentioned earlier, TaintDroid tracks the sensitive information leaving a smartphone through applications in use, notifying the user in real-time of when the information leaves and the predicted destination of the extracted information. This is done through their technology known as “dynamic taint analysis”, which relies on the tracking of data flow—data information that travels through a system of operations and has a clear end destination. On a more use-case level, TaintDroid works to notify a user about an application’s handling of personal data by sending a notification to the user after the application has been open to run. The notification appears on the homescreen, which can lead the user to a “TaintDroid Notify Detail” page, in which the types of data used is listed along with where it went. These steps are very streamlined and relatively straightforward, as the research team claims the software to be 14% more efficient than the industry standard.

While TaintDroid is useful for fast, real-time analysis of privacy-sensitive information, the solution has its drawbacks. In implementation, the current difficulty lies in that the software integration requires building a virtual firmware and flashing it into an Android device. Essentially, the installation of TaintDroid requires jailbreaking into the Android system to modify the system. TaintDroid cannot be a standalone app. Although code is all open-sourced, it requires technical Java skills to handle both the hardware and softwares associated. It is also currently limited by the operating system because it only works on Android. As for the information limitations, TaintDroid only tracks data flows and not control flows, which requires a static analysis of all the third-party applications that cannot be achieved unless all applications were open source code. This means that truly malicious players in the application industry can bypass TaintDroid's analysis by withdrawing sensitive information through control flows instead of the usual data flow. With the information being tracked, TaintDroid only notifies the user once he/she leaves the application to return to the homepage screen, and does not contain actionable functionalities for users to stop the application from taking certain pieces of data immediately [35].

MockDroid, on the other hand, is similar to TaintDroid in that it is an enhanced Android system that tracks sensitive information leaving a phone in real-time. The main addition to this software solution is that it extends options for users: not only can users track the sensitive data being accessed by running software applications, users have the ability to turn off access to any of the pieces of private information by the application (see Figure 5). The application can keep running without that specific bit of information because MockDroid implements what is called "fake permissions". Essentially, MockDroid lies to the running application by telling it that the information requested through the smartphone's databases or sensors is not present [36].



16:52

Paper Toss FREE
Backflip Studios Inc.

This application has access to the following:

Your location
coarse (network-based) location, fine (GPS) location

Network communication
full Internet access

Phone calls
read phone state and identity

22 October 2010 16:53

O2 - UK

USB debugging connected
Select to disable USB debugging.

USB connected
Select to copy files to/from your computer.

Mock permissions for application
Press to configure mocking for Paper Toss 16:53

16:54

Mocker

Paper Toss

Mocked Permissions

full Internet access

coarse (network-based) location ✓

fine (GPS) location ✓

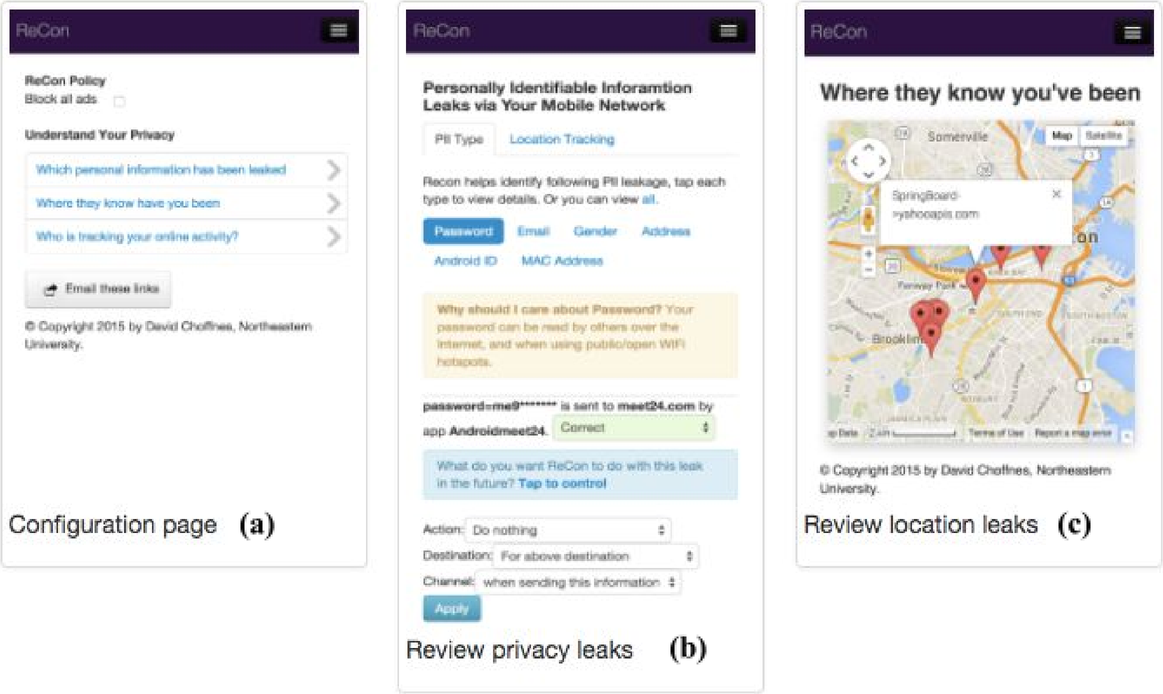
read phone state and identity ✓

Figure 5. MockDroid interface: users can track any data being accessed by software applications and can choose to turn off access to any of the pieces of private information by the application. (Image via MockDroid)

By providing users a chance to see which pieces of personally identifiable information are being accessed in real time as the application is being used, MockDroid can help the average user learn about the interactions between application services and the personal data accessed. Most smartphone application users have no idea how, when, or to what extent an app is using their private information to perform a specific function. With MockDroid, users can become more aware of personal data use on applications and learn that they can be more privacy-conscious without jeopardizing the services they need the applications to accomplish for them. This successfully tackles the problem studied by Shklovski around mobile device users and their learned helplessness around protecting personal data. If users learn that they have options to protect their personal information without giving up rights to all the services an application has to offer, then they can be trained into learning that the only choice by default is not invasion into personal information by outsiders.

Another software solution is ReCon (see Figure 6), which is in development at Northeastern University under the support of Data Transparency Lab. Unlike TaintDroid and MockDroid, ReCon has broader usage because it currently works with Android, iOS, and Windows operating systems to reveal the leaking of personally identifiable information from third-party apps (Figure 6b), including information on tracking, geographical location (Figure 6c), insecure password transmissions, and personal user information. Instead of building firmware directly into a mobile device like the two software solutions presented previously, ReCon captures the leaking mechanisms of PII through their network trace analysis, machine learning, and crowdsourced user feedback.

Their concept is based on the groundwork that personal data leaving a mobile device is transferred over the network, which can be traced by looking at the network traffic and identifying through machine learning. ReCon presents the sensitive information leaked through the network by applications via a private webpage. It provides high customizable services in that it allows users to set their own rules around how ReCon should handle the sensitive information it has identified as being jeopardized, such as options to randomize the phone identifier, broaden the location area being tracked, block trackers in app advertisements, and prevent all insecure requests from automatically coming through.



ReCon Policy
Block all ads □

Understand Your Privacy

Which personal information has been leaked

Where they know have you been

Who is tracking your online activity?

Email these links

© Copyright 2015 by David Choffnes, Northeastern University.

Configuration page (a)

Personally Identifiable Inforamtion Leaks via Your Mobile Network

Recon helps identify following PII leakage, tap each type to view details. Or you can view all.

Why should I care about Password? Your password can be read by others over the internet, and when using public/open WiFi hotspots.

password=me9******** is sent to meet24.com by app Androidmeet24. Correct

What do you want ReCon to do with this leak in the future? Tap to control

Action: Do nothing

Destination: For above destination

Channel: when sending this information

Review privacy leaks (b)

Where they know you've been

SpringBoard-
>yahooapis.com

© Copyright 2015 by David Choffnes, Northeastern University.

Review location leaks (c)

Figure 6. ReCon interface (a): users can reveal the "leaking" of personally identifiable information from third-party apps, including privacy (b) and location (c) leaks. (Image via ReCon)

Besides customization, ReCon also allows users to choose an "identical" setting so that any information being filtered through ReCon looks identical to that of several hundred other users in order to remove risks around being personally identified. Then with each privacy leak event identified, ReCon asks the users for accuracy in order to improve the machine learning mechanisms and contribute to the metadata collected of various application companies and their privacy trustworthiness. ReCon analyzes the user feedback to assign a Leakiness Score to the popular apps available to users, which is supposed to be used to give users an idea of where a particular application falls in terms of sharing private information with third-party outsiders. Apps can range from "most leaky" to "least leaky", with more leaky apps being those that are most frequently tracked as transmitting sensitive data across the network to other locations. The

Leakiness Score is available on a public webpage so that application users can have a general knowledge about an app company’s data privacy practices before opting into its services.

While ReCon provides a solution for more operating systems and has an effective way of ensuring the improvement of accuracy—according to research, its accuracy in revealing PII leaks is at 99%—the implementation of this solution is where the limitations really set in. In order to analyze traffic over a private network, the open-sourced software ReCon must be hosted on the Meddle server. Meddle is a framework that serves as an intermediary middlebox or operating system that runs on the cloud to combine virtual private networks (VPNs) with middleboxes; the server is currently in beta and requires special permission to access [38]. Once access to Meddle is granted, ReCon can be deployed from a computer system that requires a root in Linux OS. The technical knowledge required to use ReCon with personal computers is quite extensive. In addition, ReCon has two clear setbacks in network trace analysis: ReCon can only identify personal information through plaintext traffic meaning that any encrypted flows across the network cannot be detected, and it analyzes data flow without being able to account for control flow. Similar to TaintDroid, this means that if the third party application does not have its source code open, these softwares cannot implement static analysis techniques to discover how the flow of private information might be gamed by these malicious third parties. On another end in comparing with TaintDroid, ReCon does not currently offer real-time privacy violation notifications like the other solutions do [37].

Following from the concept of publicly sharing a leakiness score for each mobile application, the sensitivity score system created by Liccardi, et. al. provides for a more standard solution [39]. The system assigns a number to every app based on the amount of personal data accessed, and places it in four visible locations within the app store to inform app users: the search page, description page, update page, and the permissions page. Figure 8 shows what the modified user interface would look like upon implementing the sensitivity score system within the Google Play store and Android operating systems.

In addition to being able to clearly understand the extent of permissions the user must give up, the user can also selectively read through the the highlighted portions of the ToS and privacy policies that are relevant to their immediate privacy rights. The list of relevant sensitive permissions are flagged for the user to investigate, and will continue to remain flagged, especially since applications commonly change their ToS and their practices around collecting and using personal information. The sensitivity score system enhances the user interface of permissions requests on Android-based applications so that users can gain privacy-consciousness, in addition to increasing comprehensibility into ToS permissions and having a grounded knowledge into the trustworthiness of app companies. The increased visibility into how applications may be handling users' personal sensitive data is critical in helping them step out of initial emotional-based heuristics and prior prejudices so that they can make informed choices and best defend their privacy rights.

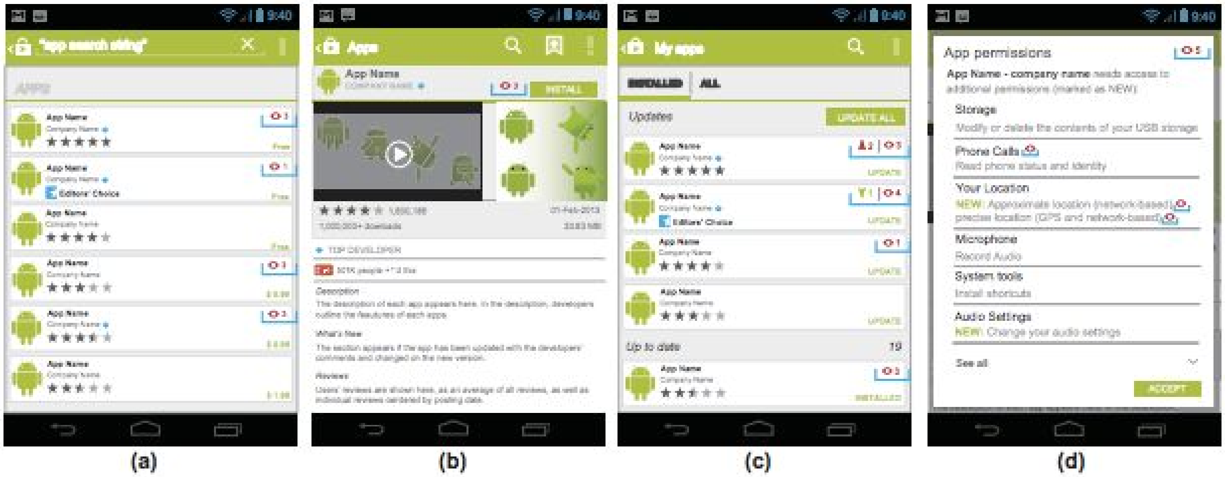
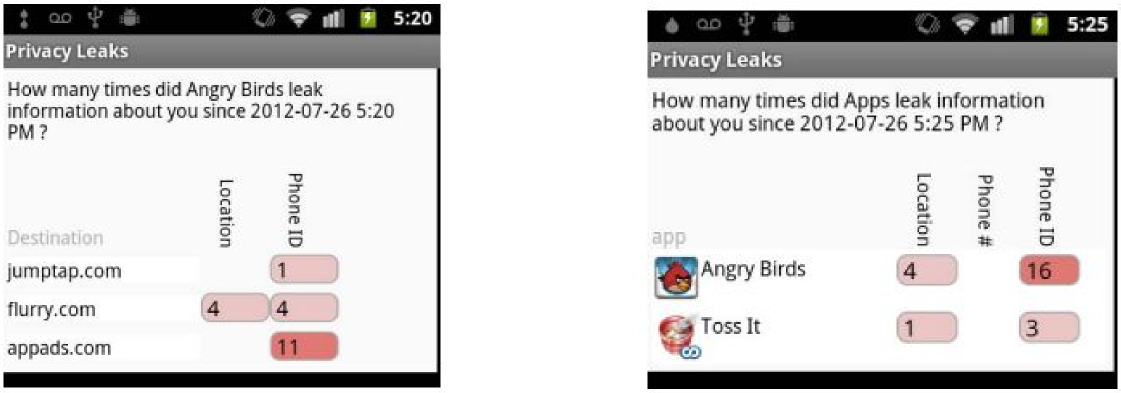


Figure 7. The sensitivity-score system assigns a number to every app based on the amount of personal data accessed, and places it in four visible locations to inform app users: (a) the app store search page, (b) the app description page, (c) the app update page, and (d) the app permissions page. (Image via CMU Journal of Privacy and Confidentiality)

While the research done around sensitivity score systems does not voice any technical drawbacks around identifying the sensitive app permissions and the personal data being accessed by the applications, current limitations include some listed from other presented solutions. The sensitivity score functionality and interface were developed over the Android operating system specifically, and also requires Google to implement the interface changes to both its app store and operating system in order to standardize the system on a large scale.

Through the research of Liccardi, et. al., it is shown that once users become more conscious of their data privacy, then they are less likely to accept the ToS and proceed to download an application. Raising privacy awareness in users may not seem like an appealing option for mobile application companies and application platforms because users are naturally more hesitant to give up data and more likely to view companies as underhanded. However, research done by Shih, et. al. show that once users have already been primed to become privacy-conscious, they are more willing to disclose personal information if they understand the terms and believe that it benefits them in the trade-off [40]. This means that if users understand which sensitive data need to be given up for certain services, then they are even more likely to follow through with trust and satisfaction of the company. This goes for all five types of users that Shih identified: privacy-conscious users, purpose-driven users, trust-based users, privacy-indifferent users, and location-sensitive users. But the current structure of informed consent through ToS and one-time popup notifications are inadequate for helping users understand privacy tradeoffs. Based on Shklovski's behavioral psychology studies, people cannot properly predict their own future behavior and plan ahead for future consent [34]. Therefore, the current system of consent is hardly enough to be considered proper informed consent for giving up sensitive personal information. The only way to remedy this problem is by implementing just-in-time disclosures. The FTC has already made recommendations for app developers around allowing express consent before the collecting and sharing of personal data with third parties through immediate disclosures and requiring affirmative express consent [13].

However, it is an immense burden to be placed on small application companies—or any application company in general—by asking them to build in their own real-time disclosures, and to ask for clear permission every time they try to collect or use a consumer's data. This issue has been tackled by Carnegie Mellon University and Microsoft, with research led by Balebako et. al. They developed Privacy Leaks, a software solution that sends out real-time notifications for users whenever their data is transmitted by an app. The information is collected into a database in the Privacy Leaks application that provides for a data visualization which summarizes the data a user has shared with a particular application (Figure 8a, 8b). In addition, the software provides clear visibility for users into the application upon download as to what specific privacy leak events are expected occur. Privacy Leaks is able to do so by collecting data from its users around the frequency of sensitive data being accessed by an application and the destination of that data.



5:20

Privacy Leaks

How many times did Angry Birds leak information about you since 2012-07-26 5:20 PM ?

Destination	Location	Phone ID
jumptap.com		1
flurry.com	4	4
appads.com		11

5:25

Privacy Leaks

How many times did Apps leak information about you since 2012-07-26 5:25 PM ?

app	Location	Phone #	Phone ID
Angry Birds	4		16
Toss It	1		3

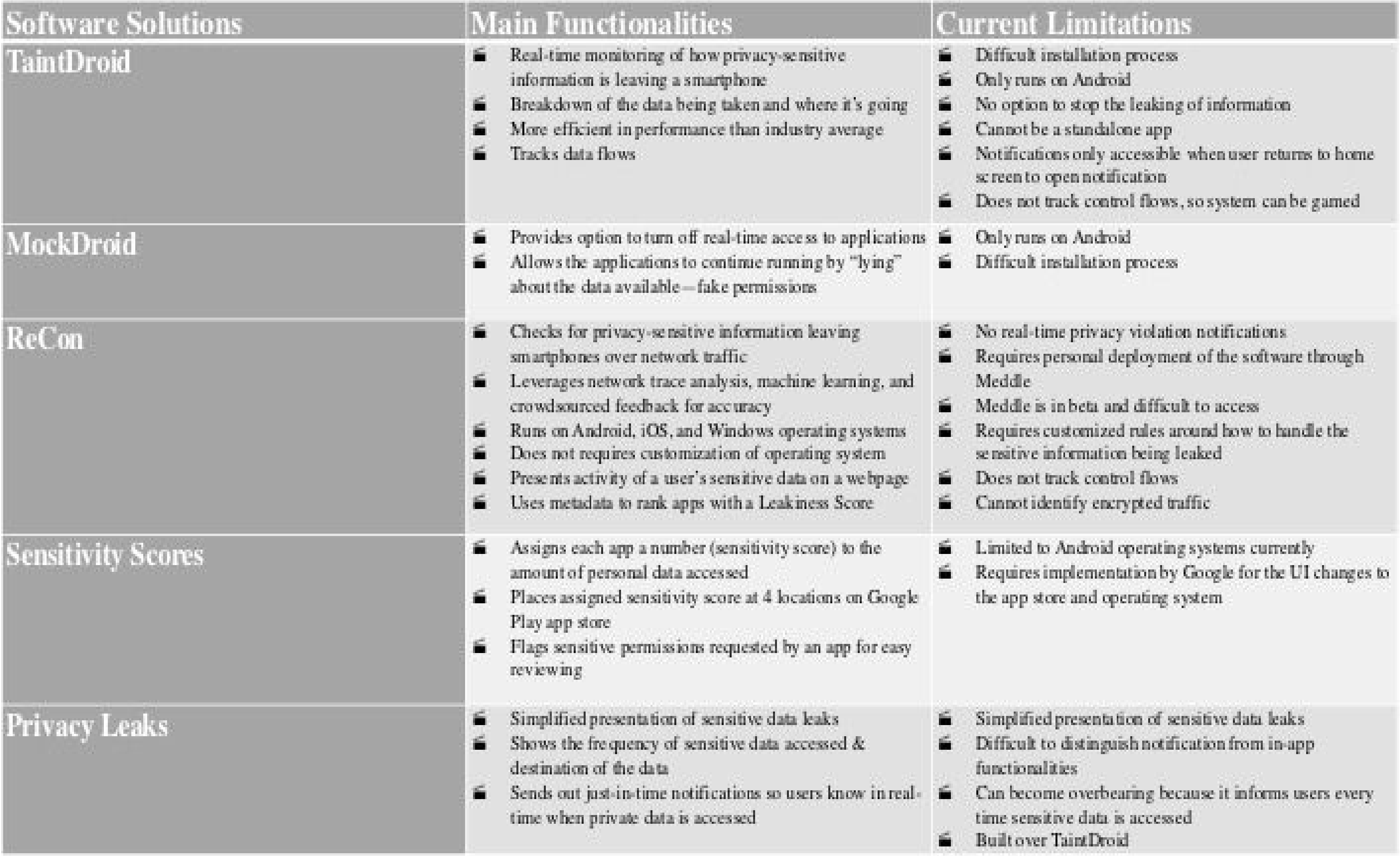
(a) Visualization dashboard of the privacy leaks

(b) Specific details as to where an app sent information

Figure 8. Privacy Leaks sends out real-time notifications every time the user's data is transmitted. (Image via Rebecca Balebako)

Strengths of Privacy Leaks revolve around its accessibility as a tool for users—the only implementation required of this technology is to download an Android app and allow it to send real-time notifications to users around private data leaks. The software presents sensitive data practices by each application company in a very manageable way; the researchers have previously prioritized which sensitive information leaks to show on the Privacy Leaks interface through focus groups. For example, a whole series of sensitive information like SIM card identifier, IMEI, IMSI, and Android ID are bunched into a category called "Phone ID" on the page. These large, simplified categories allow the average user to clearly get a big-picture into the information leaked.

On the other hand, the simplified categorization of sensitive information means that the functionality may not be enough to serve the interests of certain users who want to dig deeper into investigation of an app's data management practices. Besides presentation limitations, Privacy Leaks has notification limitations: research showed that the privacy leak sound-and-vibration-combination was difficult for users to distinguish from the running application's original functionalities, and that users may not necessarily want a reminder every time one sensitive piece of information is accessed by an application that has already been given permission acceptances. Not all the just-in-time notifications came as a surprise to users. Such software solutions should be used in a way to raise privacy awareness and equip users to make more informed decisions around providing applications with personal information without becoming overbearing. In addition, Privacy Leaks is built over TaintDroid and works by reading the data transmission events that TaintDroid tracks [41]. This means that TaintDroid’s current limitations exist for Privacy Leaks as well.



Software Solutions	Main Functionalities	Current Limitations
TaintDroid	■ Real-time monitoring of how privacy-sensitive information is leaving a smartphone ■ Breakdown of the data being taken and where it's going ■ More efficient in performance than industry average ■ Tracks data flows	■ Difficult installation process ■ Only runs on Android ■ No option to stop the leaking of information ■ Cannot be a standalone app ■ Notifications only accessible when user returns to home screen to open notification ■ Does not track control flows, so system can be gamed
MockDroid	■ Provides option to turn off real-time access to applications ■ Allows the applications to continue running by "lying" about the data available—fake permissions	■ Only runs on Android ■ Difficult installation process
ReCon	■ Checks for privacy-sensitive information leaving smartphones over network traffic ■ Leverages network trace analysis, machine learning, and crowdsourced feedback for accuracy ■ Runs on Android, iOS, and Windows operating systems ■ Does not requires customization of operating system ■ Presents activity of a user's sensitive data on a webpage ■ Uses metadata to rank apps with a Leakiness Score	■ No real-time privacy violation notifications ■ Requires personal deployment of the software through Meddle ■ Meddle is in beta and difficult to access ■ Requires customized rules around how to handle the sensitive information being leaked ■ Does not track control flows ■ Cannot identify encrypted traffic
Sensitivity Scores	■ Assigns each app a number (sensitivity score) to the amount of personal data accessed ■ Places assigned sensitivity score at 4 locations on Google Play app store ■ Flags sensitive permissions requested by an app for easy reviewing	■ Limited to Android operating systems currently ■ Requires implementation by Google for the UI changes to the app store and operating system
Privacy Leaks	■ Simplified presentation of sensitive data leaks ■ Shows the frequency of sensitive data accessed & destination of the data ■ Sends out just-in-time notifications so users know in real-time when private data is accessed	■ Simplified presentation of sensitive data leaks ■ Difficult to distinguish notification from in-app functionalities ■ Can become overbearing because it informs users every time sensitive data is accessed ■ Built over TaintDroid

3 Legal Precedents for Restricting Unfair Business Practices

Because governments enforce and lend legal authority to contracts, they also have a vested interest in making sure that the contracts they enforce are legitimate and non-abusive. There are already strong legal precedents for the government defending consumers from unfair business practices or manipulative or deceptive contracts. For example, in *Mainstream Marketing Services v. FTC,* the supreme court ruled that the FTC had the power to restrict telemarketing (through the "Do Not Call" list) because it was frequently a vehicle for abuse and unfair marketing practices. By any measure, ToS UIs employing dark patterns is an unfair and abusive marketing practice, since dark patterns are designed to trick users into checking a box without really giving informed and conscious consent. Thus, the US government should have the power and the authority to regulate ToS UIs and to eliminate dark patterns, and has a vested interest in doing so.

3.1 Legal precedents for Enforcement of ToS Contracts

While there have been no specific legislation regarding online ToS contracts, there have been many court cases regarding their enforcement. Usually, the fundamental question at stake is whether or not the user had actual or constructive notice of the content (or even the existence) of the ToS. Clickwrap agreements require actual consent, while browsewrap agreements consider the absence of dissent to be sufficient. Thus, historically, courts have been less likely to enforce browsewrap agreements than clickwrap agreements, as the former does not require the user to explicitly agree to the website's terms [22].

One recent example of a legal decision regarding a browsewrap agreement is that of *Nguyen v Barnes & Noble, Inc.*, in which the plaintiff had purchased two touchpads on the Barnes & Noble website, only to have the order cancelled due to unexpectedly high demand. The plaintiff filed a class action lawsuit for "false advertising" and "deceptive business practices". Barnes & Noble motioned to compel arbitration, on the grounds that Nguyen was subject to the arbitration agreement in their Terms of Use (ToU). The motion was denied, as the court agreed that Nguyen was not given sufficient notice of the ToU, nor did he ever agree to any of the terms. Although Barnes & Noble argued that their ToU, which was made available via a hyperlink at the bottom of every page of their website, was conspicuous enough to have given Nguyen knowledge of it, the court noted that besides the hyperlink, Barnes & Noble had not taken any other action to give notice of their ToU, and thus, held that “where a website makes its terms of use available via a conspicuous hyperlink of every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on - without more - is insufficient to give rise to constructive notice.” [23] This case is an example of a “bad” UI; not only was the ToU itself never explicitly presented to the user, but the placement of the hyperlink also impeded the user’s ability to find the ToU.

On the other hand, courts are much more likely to support the enforcement of clickwrap agreements, as indicated in Hancock v. AT&T Company, Inc. Similarly, the plaintiffs in this case argued that they were not given sufficient notice of AT&T’s ToS. However, the court sided with the defendant this time; in this case, AT&T representatives had given customers printed copies of the ToS, as well as presenting a window with the online ToS. Customers then had to click “I Acknowledge”, followed by “I Agree”, in order to finalize their purchase and begin their use of the service. The court ruled that AT&T’s explicit presentation of their ToS was sufficient notice for the customers [24].

Looking at the above cases, it is clear that current ToS contracts are often misleading, deceptive, and difficult for the reader to navigate. They are often placed in hard-to-see areas, forcing the user to look for them; even when they are explicitly presented to the user, they usually remain unread. Even more confusingly, the legal system has effectively deemed one type of ToS as enforceable and one as unenforceable, but both types of ToS are rarely read by the consumer. From one perspective, ToS contracts are mutually beneficial for both the company and the user. They allow the company to legally protect their activities (i.e. data collection), while the user gets fast access to the website and their services with just a click of their mouse. However, this provides an easy target for less scrupulous companies and websites, as shown by a recent study conducted by researchers at the University of Connecticut. In the study, participants were asked to sign up for a fictitious social networking website that included a ToS that stated, among other things, that the user’s first-born child would be given up as payment. In the end, only 2% of the 543 participants noticed the clause [25]. Clearly, it is imperative that a better system for conveying a company or website's ToS be implemented, in order to protect against possible cases of ToS abuse.

3.2 Legal Precedents for Restricting Dark Patterns

In the United States today, there is very little legislation regulating digital use of dark patterns, or obfuscating designs and UIs. However, internationally, countries have started to notice and begun regulating dark patterns. For instance, a set of guidelines of customer protections and regulations passed by the EU in 2011 contained a provision to protect against the sort of deceptive marketing practice made possible by digital commerce, including several dark pattern tactics [26]. Two years later, Britain passed a law specifically banning "sneak into basket" and "hidden cost" dark patterns [27]. Among other regulations, the British law requires buttons which commit a user to making a payment to explicitly say "I consent to paying" and outlaws pre-checked checkboxes, requiring the companies make a user intentionally check all boxes which they agree to [28].

Though these regulations are mostly to protect commercial rights and ban dark patterns which trick users into giving up money, not data, the general principle of regarding dark patterns as "scams" or unfair and deceptive practices could be extended to bans of privacy or ToS related dark patterns [29]. Though we do not recommend such a hard line approach to regulating ToS UIs, and instead support a soft-touch approach to regulation, these EU laws set an important precedent that dark patterns can and should be regulated. In order to bring American consumer protections up to the level of the EU's and to bring ourselves into compliance with international agreements and guidelines, such as the OECD recommendations and FIPPs, the United States must also adopt some sort of consumer protections against dark patterns.

3.3 FTC Guidelines and How They Relate to ToS Contracts

In the United States, there is a strong precedent of using a soft-touch approach to regulating unfair business practices and protecting consumers. Through many different regulatory bodies, the United states has taken a stand against unfair or malevolent business practices. For instance, there are consumer protections against deceptive or untrue advertising. One example can be found in the court case *Mainstream Marketing v. Federal Trade Commission,* it was ruled that it was constitutional for the government to create a "Do Not Call" list and ban telemarketers from calling any number registered on it, in order to protect citizens from abusive and deceptive advertising practices [30]. Many US regulatory bodies for consumer protections regulate using a set of guidelines, and by evaluating individual business practices on a case-by-case basis. For example, a set of guidelines for food and drug safety and evaluating the safety of each individual product which comes to market allows the FDA to flexibly regulate a huge variety of different products.

Traditionally, a similar approach has been employed by the FTC to regulate companies digital privacy practices. Rather than strict regulations on what companies may or may not do with user data, which many European countries have implemented, consumer data policy in the US is mostly regulated by the FTC using a set of guidelines and case-by-case evaluation, similar to the FDA [31]. The FTC's power to regulate consumer privacy comes from its mandate to protect against "unfair" or "deceptive" trade practices. The FTC currently regulates what sorts of data companies may collect on users, how much they can store and for how long, what sorts of protection against security breaches they must employ in order to store which sorts of consumer data, and what a company may use consumer data for. This approach to regulation has been very effective in flexibly regulating a huge number of companies which may collect consumer data for a wide variety of reasons, and protects consumers without putting to great a burden on the companies or stifling innovation [31]. Since the FTC's mission from which it gains its authority to regulate is to protect consumers from unfair or deceptive trade practices, it seems well within the jurisdiction of the FTC to not only regulate how companies can collect data, but how companies can get users to agree to data collection. In fact, a recent FTC report on privacy disclosures emphasizes the importance of companies releasing privacy information in a legible and accessible way, including "good design" and "spacing." [13] Thus, the FTC and FDA style of soft-touch regulation is the most appropriate way to protect consumers against deceitful UIs and dark patterns. The FTC, with its mission to protect users against unfair and deceptive trade practices, is a natural choice of a regulatory body and would have the authority to regulate dark patterns. For these reasons, we recommend that the FTC create and enforce a set of guidelines for UI designs around privacy contracts, in order to prevent dark patterns

Another approach to consumer protection regulation which has been effective in the United States is regulations which require certain information to be disclosed to users in an easy to understand format. One common example is nutritional information, or “Nutrition Facts,” basic information about the nutritional content of food, such as calorie content, grams of sugar, protein, fat, salt, etc, and percentages of daily values of vitamins and minerals, which must be printed on food for sale, or made available to consumers [32]. Similarly, the FTC recently released a report on data privacy disclosures, suggesting that they adopt guidelines requiring companies to disclose certain information about the data they collect and their data privacy practices [13]. This report, which explicitly compares privacy disclosures to nutritional information, recommends that companies disclose straightforward and legible summaries of their data collection practices, in was understandable to users, including making them legible, well designed and easily accessible without having bought an application. We second this recommendation, and extend it, recommending that the government support the development of software tools to help users make sense of privacy disclosures and to make ToS and privacy policies even more legible to users.

4 Proposed Solutions and Anticipated Implications

In the previous section, we set the background for FTC’s critical role in protecting consumers from deceptive trade practices. In the past few years, the FTC has done extensive work to protect consumers by trying to educate developers, software application platforms, and general mobile application consumers on the importance of digitally mobile data privacy [33]. The FTC has proposed mobile privacy policy recommendations through a recent conference with panels of multi-stakeholder experts, and has offered free resources to mobile and website businesses of any size, in order to encourage transparency of internet companies with their consumers to build up trust through protecting privacy while maintaining innovation.

However, the FTC’s current mobile privacy disclosure recommendations around the collection and distribution of data are vague, and do not offer enough support for the average small mobile application company to take the responsibility into its own hands. While there has not been a general consensus in the HCI community around standard privacy-awareness interfaces [33]—either with respect to the UI for a ToS and Privacy Policy or to technology around providing more actionable transparency to users—current HCI research all points in a similar direction. Based on the culmination of HCI research around UI improvements for privacy disclosure agreements and technology to prime user privacy-consciousness, we will make several recommendations below that the FTC can use to provide consumers, mobile application developers, and software distribution platforms with additional support and clarity around a standard format for disclosing sensitive consumer data information.

4.1 Current Recommendations on Providing Mobile Data Transparency

Through the FTC's urging for enhanced mobile privacy protections, the National Telecommunications and Information Administration (NTIA) has developed a voluntary privacy code of conduct for application developers and publishers, which the FTC has announced to "view favorably in connection with law enforcement work". This includes proposed standards for UI design, language, and links around the implementation of short form notices to provide users with greater transparency around sensitive data usage and protection [34]. NTIA's work reflects the types of regulations the FTC currently has in place—voluntary, intricately detailed yet broad and quite difficult to navigate in application, and containing few resources for actual execution.

On other fronts, private organizations such as boot camps, developer conferences, privacy summits, and workshops are trying to work with the FTC in providing guidance for developers and platforms on how to build trust with consumers through digitally mobile data transparency. As for the privacy policy recommendations laid out for mobile software application companies through the FTC's Privacy Report, it asks developers to build with privacy in mind, simplify consumer choice by providing privacy options in context, heighten transparency with app consumers by disclosing additional details about the collection and use of sensitive personal information, limit data collected to only those necessary for the requested service, and to collaborate with other data collection companies to provide greater privacy disclosures that are standard and compatible with small mobile screens.

Not only that, the FTC goes deeper by recommending that software application distribution platforms like Apple, Google, Amazon, Microsoft and Blackberry should alter the UI of their app stores and leverage their application programming interfaces (APIs) to promote just-in-time disclosures and privacy dashboards for consumers [13]. Since apps must integrate with the app stores' APIs in order to collect standard categories of a user's information on a mobile device, the FTC is placing much pressure on distribution platforms to hold individual app companies accountable for better data privacy transparency and practices. But a problem here is that these platforms cannot control the data being collected, accessed, and transported on an individual-app level; the distribution platforms can only track what information is being collected from the users by the apps through APIs as a whole, but not which sensitive information the app is taking directly or sharing with third party outsiders such as advertisers or app analytics tools. Because of this technological barrier, we should not rely predominantly on large software application distribution platforms to do the heavy-lifting when it comes to policing the digitally mobile companies to protect consumer mobile data and provide transparency.

While the recommendations of FTC would indeed protect privacy, trust, and innovation at the same time, they are highly unlikely to be addressed by both large distribution platforms and also small mobile application companies that are tight on resources and might not have consumer data privacy as the utmost priority. Essentially, the FTC is asking a lot from small mobile app companies, and has provided a very small basis of support or clarification. Most of the third-party resources that FTC is helping build are not currently accessible to the average mobile application business; in addition, the FTC has admitted to difficulties in communicating these policy recommendations with all application companies across the US [13]. Because of these difficulties, it is important that we list out recommendations that provide greater clarity as to what exactly a standard ToS should look like, with respect to informing consumers about the company's practices around collection and use of sensitive personal data, and how the FTC can go about building upon our initial presented points based on HCI research. Afterwards, we will address how a synthesized combination of current HCI technology software can be leveraged to raise privacy-awareness in app users.

4.2 Creation of a Standardized Template for ToS

Our first recommendation is that the FTC assemble a panel of experts to create a set of usability guidelines for creating straightforward, non-deceptive UI designs, and require that companies abide by these guidelines in UI designs related to ToS contracts, especially contracts related to privacy. We suggest that the FTC create this set of usability guidelines by assembling a panel of unbiased (non-corporate-associated) experts in human-computer interactions and UI design. Though we recommend that the actual creation of a set of usability guidelines be left to this panel of experts, we present several broad guidelines or starting points for experts looking to create such a set of guidelines:

A. Consistency: We recommend that the FTC guidelines mandate some sort of consistency between ToS UIs,and between multiple pages in a single UI, whether strongly enforced through a strict template (such as nutrition facts labels) or through some sort of looser template. Consistency should include formatting, use of colors, use of terminology, and function of similar looking objects. This will prevent users from being confused when transitioning from one UI to another and dark patterns which rely on users making assumptions based on UIs they are familiar with. It also makes it easier for users to navigate many ToS UIs once they have been exposed to one, rather than forcing them to navigate an entire new system for each contract they agree to. Thus, consistency will lead to better readability and usability, and will encourage readers to engage with each ToS by removing the technical barrier of familiarizing themselves with a new UI.

B. Honest direction of attention and formatting: We recommend that the FTC guidelines mandate good formating which contributes to readability and directs attention towards key privacy related details. Typesetting and color should be used to create visual hierarchies, drawing the user's eye to essential information, and designers should always treat content of the ToS document, especially clauses having to do with specific data to be collected and specific uses of data to be collected, as essential information. All option the users are presented with should be represented equally, in equally sized fonts and similar locations on the page. Formatting should not be used to direct user attention away from essential information. These formatting guidelines will encourage users to familiarize themselves with the ToS, will make it easier for users to find privacy related information, and will defeat dark patterns which depend on making users overlook information or options.

C. Transparency and Feedback: The state of a user's privacy setting should always be obvious from the interface to the user, and all changes made to privacy settings should be clearly reported. Preferably, UIs should indicate when data is being collected and what sort is being collected through obvious icons or popups. Privacy settings should be easy to locate, either on the app's homepage or in an easy-to-find menu. The UI should clearly report when privacy settings are changed by a user, and should make it clear when a user has attempted to and failed to change privacy settings. These guidelines would prevent dark patterns, which make it unclear to users which data is being collected, and trick them into thinking they have changed their privacy settings when they have not.

D. User Control and Undo Options: A good interface should make it easy for a user to change their privacy options and undo any accidental or unwanted choices. Privacy settings should be easy to locate, located together in the same clearly labeled menu, and not nested too deep in with other settings. Users should be presented with a clear undo option for any choice they make which does not require them to expend significantly more effort than making the choice in the first place. These guidelines will prevent forced continuity dark patterns which make it much harder for users to undo choices, as well as hidden menu dark patterns like the iOS 6 example discussed above, which make it inconvenient to change settings from defaults.

We believe that these guidelines would prevent some of the most egregious and most commonly used dark patterns employed in user interactions with privacy, such as hidden menus, trick questions, and other obfuscations and misdirections. These guidelines would make UIs relating to ToS and privacy settings more comprehensible, straightforward and easier to use for consumers, and would eliminate opportunities for dishonest concealing of information and manipulation of users. Therefore, we recommend that the FTC assemble a panel of experts in HCI and UI design to flesh out these principles and create a set of guidelines or loose template to promote usability and prevent abuses.

We believe that this proposal will protect the interests of users better than other possible frameworks for preventing dark patterns. For example, when compared the the UK framework of specifically banning specific dark patterns, our proposal is more flexible and comprehensive; whereas restricting specific dark patterns requires legislators to stay on top of every deceptive UI trick which is invented, providing a positive set of guidelines ensure that the regulation will be effective at preventing deceptive UIs no matter what new dark patterns are invented. Similarly, regulating with a set of guidelines and a soft touch solution allows for more flexibility and more opportunity for regulating bodies like the FTC to decide on a case by case basis, which is important in a subtle and subjective field, such as usability of terms of service. A set of guidelines would allow the FTC to better assess UIs in the gray area while still giving companies a good idea of which UIs will be considered dark patterns and which will not. Thus, we believe it to be a better solution than setting hard regulations on UIs through legislation, because it allows for more comprehensive and flexible regulation of new dark patterns and for negotiating the ambiguities and subtleties of UI design. Finally, since many guidelines for preventing dark patterns are also simply good principles of UI design, we believe that creating a set of guidelines will encourage companies to create more usable, intuitive and simple UIs, and overall improve user experiences with apps. For these reasons, we believe that this policy will be the most effective in protecting users from deceptive practices, and thus is in the best interests of users, and the government, which wishes to protect them.

Though it may be argued that our proposal will hurt businesses, especially the ability of small businesses to break into the market, we believe that our proposal will actually help small business enter the marketplace and promote innovation. The counter-argument runs that limiting the ability of new businesses to employ dark patterns or deceptive UI designs in order to grow their brand and audience will give companies which became established through the use of dark patterns an unfair advantage over new companies entering the marketplace. Thus, the fear is that our proposal would stifle innovation while promoting companies which reached their current status through the sort of unfair business practices which we aim to regulate in the first place. However, we argue that our proposal will actually help new businesses, especially small businesses, by removing legal burdens from them. The FTC providing a clear set of guidelines for usability will allow small businesses entering the market to simply follow the template, saving them fears about liability and the costs of hiring lawyers to create usable and enforceable terms of service. In fact, the guidelines would be doing companies work for them, making it easier for them to draft up an enforceable ToS and enter the marketplace. Furthermore, because there is much overlap between good UI design and non-deceptive UI design, the FTC will be providing guidelines which will help emerging businesses develop good UIs, improving their product as well as user experience. This is another advantage of our proposal over the UK solution of directly banning certain dark patterns, which still puts the burden on companies to make sure that they are avoiding banned dark patterns while providing them no tools to make better UIs.

Secondly, we argue that, while our proposal may require some companies to change their business practices, it will also open up new markets for competition and will give advantages to companies with good user data privacy practices. Many companies are likely worried that restricting the range of possible UIs for user privacy agreements will hurt their business, depict their privacy practices in a less favorable light, and prevent them from using strategies which have contributed to their growth and success. However, we argue that our proposal will not hurt business in general, as it will open new markets for competition and will advantage companies with good consumer privacy data practices. With the current state of ToS and levels of obfuscation in user data privacy practices, it is very difficult of companies to gain an advantage by having better data privacy practices, because it is very difficult for users to determine what companies' privacy practices actually are, and it is easy for companies with poor data privacy practices to masquerade as having good data privacy practices. However, with less obfuscated ToS created following a set of usability guidelines, it will be easier for users to distinguish between companies with good and bad data privacy practices, and to actually make choices based on these facts. Thus, our proposal will give an advantage to companies with good data privacy practices, allowing them to compete with other companies based on their privacy practices, and to attract the business of privacy conscious users.

4.3 Development of New Software Solutions to Elucidate ToS

While all the software technology created by HCI researchers that we presented above in Section 2.3 have their drawbacks, they all provide little parts that can be immensely powerful when synthesized together into a tool for promoting privacy-awareness in users of digitally mobile devices. Based on the established HCI research, we have put together a comprehensive toolkit that can best be used to help the average user learn about privacy. The toolkit is called the Privacy Awareness Kit, and consists of a combination of Sensitivity Scores, TaintDroid, MockDroid, ReCon, and Privacy Leaks. This Kit has the various softwares working together to make up for set limitations and provide for the most effective, efficient, and simple solution for users. Our recommendations around implementation of the Privacy Awareness Kit are geared predominantly towards operating systems companies such as Google, Microsoft, and Apple, along with major mobile software distribution platforms such as Google Play, App Store, Windows Store, etc., with recommended oversight by the FTC. However, these policies are meant to be read by the average user of digitally mobile devices so that everyone has a clear understanding as to where the Kit is coming from.

The Privacy Awareness Kit takes the scattered pieces of substantial HCI research and puts it together into one package that can be implemented to promote privacy-consciousness in all users. Based on our previous discussions, TaintDroid and MockDroid are useful for real-time monitoring of sensitive data leaving a mobile device. However, they require difficult installation processes and only work on Android operating platforms. In the Kit, TaintDroid and MockDroid would be combined in order to give users real-time feedback on private information being accessed by applications and provide users with options to turn off certain sensitive permissions without turning off the entirety of the application's functionalities. The open source code of those softwares would then be integrated into ReCon, which provides for similar functionalities of tracking sensitive data use by applications as TaintDroid and MockDroid, but goes a step further in accuracy levels and operationality on all major operating systems. ReCon uses network trace analysis and machine learning in order to achieve high levels of accuracy in detecting privacy leaks. However, the software currently must be hosted on a beta middlebox known as Meddle. Because of this, our recommendation for the Kit requires the ReCon and Meddle development teams to open up Meddle to public beta so that the bundle of tools can be leveraged. We recommend that the FTC work further with these development teams to provide necessary resources and support to refine Meddle and move it out of beta into full product. As for these three softwares around tracking sensitive data leaks that are part of the Privacy Awareness Kit, our recommendation is for the FTC to work directly with all major operating systems companies to implement these directly into the operating systems' internal codes. This would mean that any digitally mobile device running on the major operating systems would have this bundle of real-time privacy tracking tools immediately available for the user to access under "Settings" and "Privacy" tabs. We recommend the FTC to take an initial soft touch approach upon the regulation of this, since most major operating system companies have already voiced their concerns of data protection and support for promoting data privacy awareness for the average user [43][44].

A more direct regulation to be made by the FTC would be ban of using control flows to collect sensitive information from users through applications. Since all the software solutions presented by current HCI research shows that it is virtually impossible to track sensitive data leaks from applications through control flows, which would require having access to the source code for applications, the FTC should work to ensure that applications abide to the standard industry practice of accessing sensitive data through data flows. We recommend that the FTC take actionable measures around these practices by creating rules that explicitly ban the use of control flows to collect information through applications, and declare it to be a deceptive business practice. This authority is given by the provision under Section 18 of the FTC Act, 15 U.S.C Sec. 57 [45].

As for the rest of the Privacy Awareness Kit, consisting of the Sensitivity Scores system and Privacy Leaks app, we recommend that the FTC work with the operating system companies and software distribution platforms to incorporate them. For the devised Sensitivity Scores interface, the FTC could strongly encourage major software distribution platforms to incorporate them into the app store user interfaces. A streamlined standardization between all major platforms could occur through a special discussion hosted by the FTC, inviting all the major stakeholders from the major software distribution platforms, HCI researchers, and experienced UI designers to contribute. With this precedence, other software distribution platforms can follow the lead easily by incorporating the well-tested Sensitivity Score system into their own services. On a level deeper, these standards will encourage software application businesses to hold themselves more accountable for the amount and types of sensitive permissions requested and accessed. And then on a personal front, the standardized Sensitivity Scores will allow the average user to make more informed decisions about releasing personal information and learn to navigate ToS and Privacy Policies more easily.

The Privacy Leaks application provides for the type of just-in-time notification that the FTC is currently recommending to mobile companies and mobile device users. Therefore, we recommend that Privacy Leaks be installed as a default app for any smartphone. This may be achieved through the FTC's support around the major operating systems configuring Privacy Leaks into a standard application. By doing this, the burden of just-in-time notifications for privacy leaks do not have the fall into the hands of the independent app developer. In fact, this default of notifying users every time an application is withdrawing sensitive data means that application companies will become more discretionary and limit the amount of data collected to only the bare minimum, in order to stay competitive and maintain trust with the users. And since Privacy Leaks is currently built over TaintDroid, which we recommend to be integrated with

ReCon and MockDroid, this particular recommendation is only effective through the integration of the entire Privacy Awareness Kit.

In summary, we recommend the Privacy Awareness Kit to be used as a package, because it contains essential pieces of extensive research-based technology that is a powerful solution when implemented as a whole. The combination of TaintDroid, MockDroid, ReCon, Sensitive Scores, and Privacy Leaks is an empowering tool for all users to easily learn about data privacy and how to place that responsibility back into their own hands.

5 Conclusion

As mentioned previously, the issues addressed in this paper are relevant to three main categories of stakeholders: the users, the government and the businesses, both large and small. Our proposal will strongly benefit the users by providing them with more comprehensible and readable ToS contracts, as well as giving them software tools to inform themselves about a company's privacy policies. Additionally, we believe that the users deserve the most priority with regards to policy-making, as they are the least well-equipped to protect themselves and their rights. Ultimately, it is the government that has the final say in most decisions. However, companies still have more legal expertise and resources at their disposal than the average user.

Our proposal will also satisfy the government, as all the advantages that are provided to users are also available to the government. Standardizing ToS contracts will especially facilitate the process of evaluating them and deciding whether or not they are constitutional or enforceable, which would allow the government to better serve the needs of the users and companies.

Lastly, our proposal will benefit businesses, especially smaller businesses. A standard ToS template would reduce the legal and financial strain upon small companies, allowing them to focus their resources on creating and innovating better products. Furthermore, a company with good privacy practices could incorporate the information provided by the software tools in their current marketing strategies. For example, a business with a good 'privacy score' could tie the score to their brand, which would add even more value to their product.

6 Bibliography

1. Dark Patterns: Fighting user deception worldwide. (n.d.). Retrieved November 27, 2016, from http://darkpatterns.org/
2. Mcdonald, A. M., Reeder, R. W., Kelley, P. G., & Cranor, L. F. (2009). A comparative study of online privacy policies and formats. Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. doi:10.1145/1572532.1572586
3. OECD guidelines on the protection of privacy and transborder flows of personal data. (2013). Paris: Organisation for Economic Co-operation and Development.
4. Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015. (2015). Retrieved November 28, 2016, from https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf
5. Enck, W., Gilbert, P., Chun, B., Cox, L. P., Jung, J., Mcdaniel, P., & Sheth, A. N. (2014). TaintDroid. Communications of the ACM Commun. ACM, 57(3), 99-106. doi:10.1145/2494522
6. Infographic: The Average Smartphone User Has Installed 26 Apps. (2013). Retrieved November 28, 2016, from https://www.statista.com/chart/1435/top-10-countries-by-app-usage/
7. Waddell, T. F., Auriemma, J. R., & Sundar, S. S. (2016). Make it Simple, or Force Users to Read? Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16. doi:10.1145/2858036.2858149
8. Fiesler, C., & Bruckman, A. (2014). Copyright terms in online creative communities. Proceedings of the Extended Abstracts of the 32nd Annual ACM Conference on Human Factors in Computing Systems - CHI EA '14. doi:10.1145/2559206.2581294
9. Readability - Clear Language Group. (n.d.). Retrieved November 28, 2016, from http://www.clearlanguagegroup.com/readability/
10. Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. (2012). Washington: The White House.

11. Rainie, L. (2016). The state of privacy in post-Snowden America. Retrieved November 28, 2016, from http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/
12. Rainie, L., & Duggan, M. (2016). Privacy and Information Sharing. Retrieved November 28, 2016, from http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/
13. U.S.Cong. (2013). Mobile privacy disclosures: Building trust through transparency [Cong.]. Washington, D.C.: Federal Trade Commission.
14. Goel, V. (2014, June 29). Facebook Tinkers With Users' Emotions in News Feed Experiment, Stirring Outcry. Retrieved November 28, 2016, from http://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html
15. Fung, B. (2014, January 3). Snapchat Stays Mum about Breach. The Washington Post. Retrieved 2016, from http://www.highbeam.com/doc/1P2-35540580.html?refid=easy_hf
16. Fischer, B. (2011, June 4). CEOs Say Innovation Is Most Important Factor For Growth. Retrieved November 28, 2016, from http://www.forbes.com/sites/billfischer/2011/06/04/ceos-say-innovation-is-most-important-factor-for-growth-voxy-co-nz/
17. Jones, T. (2010, April 29). Facebook's "Evil Interfaces" Retrieved November 28, 2016, from https://www.eff.org/deeplinks/2010/04/facebooks-evil-interfaces
18. Brignull, H. (2013, August 29). Dark Patterns: Inside the interfaces designed to trick you. Retrieved November 28, 2016, from http://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you
19. Nielsen, J. (1995, January 1). 10 Heuristics for User Interface Design: Article by Jakob Nielsen. Retrieved November 28, 2016, from https://www.nngroup.com/articles/ten-usability-heuristics/
20. User Interface Design Basics. (n.d.). Retrieved November 28, 2016, from https://www.usability.gov/what-and-why/user-interface-design.html

21. Martin, S. (n.d.). Effective Visual Communication for Graphical User Interfaces. Retrieved November 28, 2016, from https://web.cs.wpi.edu/~matt/courses/cs563/talks/smartin/int_design.html
22. Brehm, A. S., & Lee, C. D. (2015, January). From the Chair: "Click Here to Accept the Terms of Service". Communications Lawyer, 31(1).
23. Nguyen v Barnes & Noble, Inc., 763 F.3d 1171 (9th Cir. 2014)
24. Hancock v. American Telephone & Telegraph Company, Inc., No. 11-6233 (10th Cir. 2012)
25. Poitras, C. (2016, August 18). The Privacy Paradox - UConn Today. Retrieved November 28, 2016, from http://today.uconn.edu/2016/08/privacy-paradox/
26.
27. Brignull, H. (2014). Some Dark Patterns now illegal in UK – interview with Heather Burns | 90 Percent Of Everything. Retrieved November 28, 2016, from http://www.90percentofeverything.com/2014/08/26/some-dark-patterns-now-illegal-in-uk-interview-with-heather-burns/
28. Noel, J. (2014, January 27). Is UK retail ready for new EU directive? – The Guardian. Retrieved November 28, 2016 from https://www.theguardian.com/media-network/media-network-blog/2014/jan/27/retail-eu-consumer-rights-directive
29. The Directive on Consumer Rights. (2016, November 24). Retrieved November 28, 2016, from http://ec.europa.eu/consumers/consumer_rights/rights-contracts/directive/index_en.htm
30. Mainstream Marketing Services, Inc. v. FTC, 283 F. Supp. 2d 1151 (D. Colo. 2003)
31. Solove, D.J. & Hartzog, W. (2013, August 15). The FTC and the New Common Law of Privacy. 114 Columbia Law Review 583. Retrieved November 28, 2016, from https://ssrn.com/abstract=2312913
32. Labeling & Nutrition. (n.d.). Retrieved November 28, 2016, from http://www.fda.gov/Food/IngredientsPackagingLabeling/LabelingNutrition/default.html

33. Privacy Through Awareness — Introducing Real-Time Feedback – Privacy Observatory Magazine (2016). Retrieved November 28, 2016, from http://www.privacyobservatory.org/privacy-through-awareness-introducing-real-time-feedback

34. "Privacy Multistakeholder Process: Mobile Application Transparency." *Privacy Multistakeholder Process: Mobile Application Transparency | NTIA*. N.p., 12 Nov. 2013. Web. 08 Dec. 2016.

35. Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014, May 1). Leakiness and creepiness in app space. *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems - CHI '14*. doi:10.1145/2556288.2557421

36. Enck, W., Gilbert, P. & Chun, B. (2010). TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. In Proc. Of the USENIX. Retrieved November 28, 2016, from http://www.appanalysis.org/tdroid10.pdf

37. Beresford, A.R., Rice, A., Skehin, N. & Sohan, R. (2011). MockDroid: trading privacy for application functionality on smartphones – HotMobile. Retrieved November 28, 2016, from http://www.cl.cam.ac.uk/~arb33/papers/BeresfordAREtAl-MockDroid-HotMobile2011.pdf

38. C. (2012). Services - ReCon: Take Control of Your Mobile Privacy: Services Provided. Retrieved November 28, 2016, from https://recon.meddle.mobi/services.html

39. C. (n.d.). Meddle: Take Control of Your Mobile Traffic. Retrieved December 07, 2016, from https://www.meddle.mobi/

40. Liccardi, I., Pato, J., Weitzner, D. J., Abelson, H. & Roure, D.D. (2014). No technical understanding required: Helping users make informed choices about access to their personal data - Mobiquitous. Retrieved November 28, 2016, from http://people.csail.mit.edu/ilaria/papers/LiccardiMobi.pdf

41. Shih, F., Liccardi, I. & Weitzner, D. J. (2015). Privacy Tipping Points in Smartphones Privacy Preferences - CHI. Retrieved November 28, 2016, from http://people.csail.mit.edu/ilaria/papers/ShihCHI15.pdf

42. Balebako, R., Jung, J., Lu, W., Cranor, L. F. & Nguyen, C. (2013). “Little brothers watching you”: raising awareness of data leaks on smartphones - Proceedings of the Ninth Symposium on Usable Privacy and Security. Article No. 12. Retrieved November 28, 2016, from http://delivery.acm.org/10.1145/2510000/2501616/a12-balebako.pdf?ip=174.63.83.98&id=2501616&acc=PPV&key=4D4702B0C3E38B35%2E4D4702B0C3E38B35%2EFAABE9AE10A12EF0%2E4D4702B0C3E38B35&CFID=227533&CFTOKEN=85314920&__acm__=1480209983_27f4138e08d8621feb8c0c5221eea35b
43. "Privacy - Apple." *Apple*. N.p., n.d. Web. 08 Dec. 2016.
44. "Privacy Policy – Privacy & Terms – Google." *Privacy Policy – Privacy & Terms – Google*. N.p., n.d. Web. 08 Dec. 2016.
45. "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority." *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority | Federal Trade Commission*. N.p., July 2008. Web. 08 Dec. 2016.