New Paradigm or Ethics Washing?

An Analysis of Facebook's Ethics Report

Katherine O'Keefe; Daragh O Brien
CASTLEBRIDGE

Castlebridge | Invent Centre, DCU, Glasnevin, Dublin 9 | www.castlebridge.ie

Table of Contents

INTRODUCTION

"Action is indeed the sole medium of expression for Ethics" -- Jane Addams

In June, Facebook in partnership with consultancy Ctrl-Shift published a very interesting report on "A New Paradigm for Personal Data", promoting a shift to a more user-"sustainable" and even ethical approach to personal data. The report, built from roundtable conversations held with experts across Europe, the Americas, and Asia-Pacific proposes some interesting ethical statements and standards. This report in conjunction with recently introduced new products and changes to existing products by Facebook presents an interesting case study in why we focus on outcomes at Castlebridge.

In a sense, Facebook's new report is acting as advertising for Facebook as a company, selling the impression that Facebook cares about user privacy. Facebook's messaging in the Ctrl-Shift report is generally consistent with their stated values listed on Facebook's website, creating a unified message that Facebook is an ethical organization that cares about preserving your privacy. However, this report and messaging in conjunction with actions and new projects recently announced by Facebook serve as an object lesson in how, "Action is indeed the sole medium of expression for Ethics". While the messaging Facebook has is consistent with the "new paradigm" suggested in the report, the actual outcomes of Facebook's recently revealed projects and changes to policy seem to belie this message. This results in a concerning disconnect between expectations engendered by Facebook's public statements, their stated ethical standards, and the outcomes of their processes and products.

OUTCOMES VERSUS EXPECTATIONS

While we find much of value expressed in the Facebook-led report, much of it is not in fact new. When it comes to data and information management, the principle of quality data is key. And the fact is, when it comes to personal data, trust goes both ways. To be able to trust that people will give you personal data that is of the quality you as an organization require, you need to be able to demonstrate that you can be trusted with personal data.

Privacy by design stipulates that privacy is not a zero-sum game. But rather, processes with privacy built in from the beginning can be a win-win (a.k.a. sustainable) model. This model requires consideration of the individual's objectives, expectations, and requirements in the exchange of information, and the engineering of the proposed processing activities in a manner that addresses the "win-win" objective inherent in the Privacy by Design ethos.

"Privacy" becomes a quality characteristic of data and of the processing activities that act on that data. In that context, the expectation of the individual whose information you are processing of how their privacy will be respected, and the level to which that expectation is met, constitutes a key element of the trust that individuals have in your brand, your use of their data, and your organisation.

An organization that builds its business model on the willingness of individuals to share their personal data with the organization depends on a relationship of trust between the organization and the individuals whose data the organization processes. If individuals lose trust in the organization's good will or ability to respect their data and their autonomy, they are likely to stop sharing their data. This may indeed already be happening for Facebook, as it is facing a decline in users sharing content about their personal lives.[1]

While the "new paradigm" that Facebook promotes may have laudable aspects, perhaps it would be more productive to consider a new business model for processing personal data. To create a sustainable business model for quality processing of personal data, it is imperative to ensure that the outcomes of your processes match the expectations of your customers, whether internal or external.

A Conceptual Framework for Executing Ethics and Privacy

In a previous paper we discussed a framework for implementing Ethical Information Management in an organisation. This framework addresses the alignment between the ethical framework of the organisation (as espoused in its organisation culture and internal social norms), the ethical framework of society, and the internal operative models for strategy, governance, and execution within the organisation. This model is derived from the 9-Box "Amsterdam Model" developed by Professor Rik Maes in the University of Amsterdam.

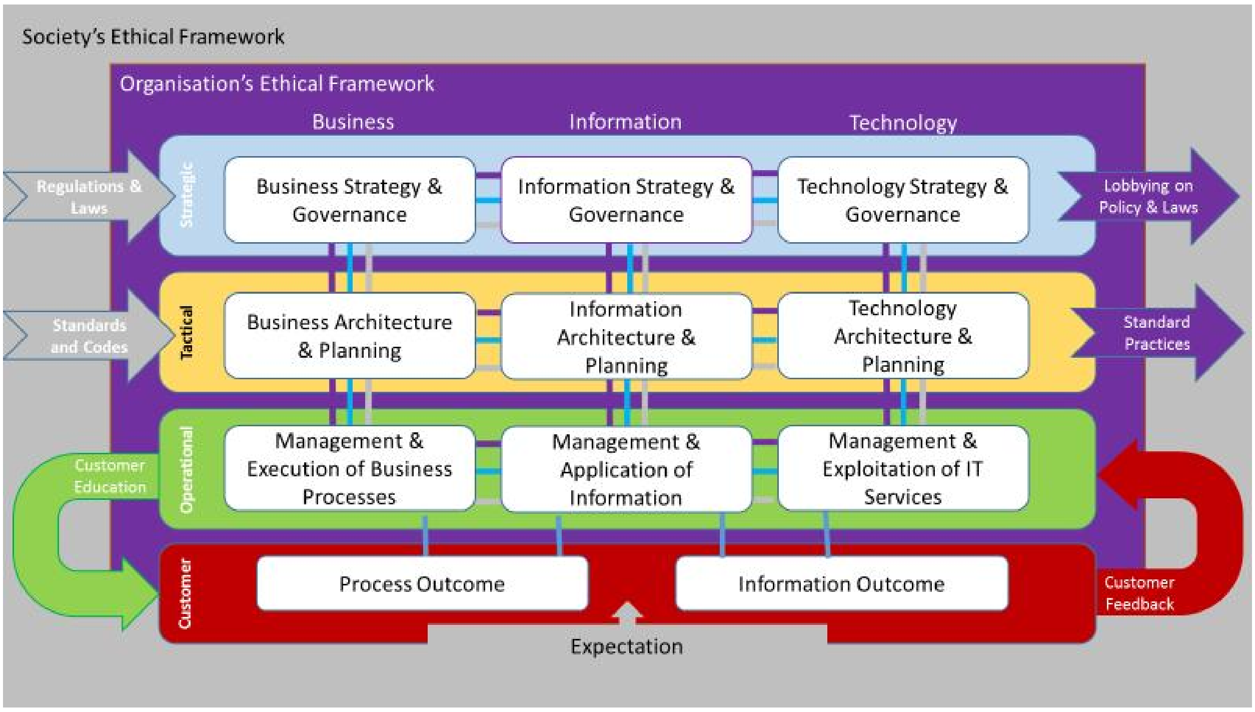

Society's Ethical Framework
Organisation's Ethical Framework
Business
Information
Technology
Regulations & Laws
Strategic
Business Strategy & Governance
Information Strategy & Governance
Technology Strategy & Governance
Lobbying on Policy & Laws
Standards and Codes
Tactical
Business Architecture & Planning
Information Architecture & Planning
Technology Architecture & Planning
Standard Practices
Customer Education
Operational
Management & Execution of Business Processes
Management & Application of Information
Management & Exploitation of IT Services
Customer
Process Outcome
Information Outcome
Customer Feedback
Expectation

Figure 1 The Castlebridge E2IM Framework

In summary, this framework describes the relationship between society's ethical framework and expectations, the ethical framework of the organisation, and the functional activities at an operational, tactical, and strategic level in an organisation that influence the process outcomes (i.e. delivery of a product or service) and information outcomes (i.e. uses of, processing of, or distribution of personal or other data). Society influences the organisation through laws, standards, and customer feedback. The Organisation influences society

[1] *Efrati, Amir. "Facebook Struggles to Stop Decline in 'Original' Sharing". The Information. 7 April, 2016 https://www.theinformation.com/facebook-struggles-to-stop-decline-in-original-sharing (accessed 31 August, 2016)*

though lobbying, development of "standard practices", and engaging in customer education. Within the organisation, formal governance and control structures over the Business, Information, and Technology functions of the organisation are influenced by the ethical drivers of society and of the organisation which guide the actions of individuals within formalised governance or procedural rules.

Facebook's stated values and the Facebook/Ctrl-Shift report emphasize how important it is that customers should be educated, and should have control over their data (both an Information and a Process outcome in the Castlebridge framework). The stated values create an expectation on the part of customers, and by extension society, as to the conduct of Facebook in the context of the processing of personal data. The actual outcomes of Facebook's business processes, however, do not fit these values.

When there is a disconnect between customer expectations as influenced by an organization's public message and the outcomes of their processes, it is likely that that organization will be seen as unethical or untrustworthy, even if they have the best of intentions. Their information and processes cannot be trusted because the delivered product does not meet or exceed expectations. In this context, we have a divergence between what we term the "Statement of Ethic" and the "Action of Ethic" (i.e. the actions of the organisation)

Complaints are a way in which customers express their perception of the disconnect between outcomes and expectations. Customers may also use complaints to redress a perceived power imbalance. Complaints to the organization itself may be a very useful warning to the organization that the outcomes of its processes as communicated to the public do not match their customers' expectations, and there may be a breakdown in communication or in the process itself. At this stage, the organization has a chance to address breakdowns in communications and processes to develop mutually beneficial outcomes and relationships. If an individual perceives that an organization is unwilling to engage with them in this way or is exploiting an imbalance in power, they may exercise their power to complain to the regulator, triggering the regulatory influence of society's ethical framework to put pressure on modifying the actions and ethical framework of the organization.

While outside the core scope of our Ethical Enterprise Information Management Framework, the feedback mechanism of complaints as a check and balance that aligns the processing of information by organisations with the wider ethical norms of society highlights the importance in this dynamic of effective Regulatory mechanisms that can act independent of other social or societal forces (e.g. lobbyists, legislators, or litigation). It is only when Regulators can be relied upon by individuals to act independently and to uphold, at a minimum, the rules which have been legislated for by society's elected representatives that there is an effective constraint on action and restraint on unethical activity. This is explicitly recognised in EU law and is implicit in the actions of the FTC on privacy issues.

We explore the nature of the disconnect between the "Statement of Ethic" and the "Action of Ethic" in the rest of this paper.

WORDS: ETHICAL THEMES IN FACEBOOK'S NEW PARADIGM

False Logic of the "Trade-Off"

Stephen Deadman, Facebook's Chief Privacy Officer clearly denies the "trade-off thinking" that innovation with data is incompatible with preserving "individuals' rights to privacy and self-determination", calling this viewpoint entrenched by both policy makers and industry innovators. This is an attitude he calls out as limiting, undesirable, and unnecessary, leading to "*suboptimal outcomes*".[2]

We absolutely agree with Deadman that the "trade-off" rhetoric is false logic, and that so-called dichotomies such as Privacy/Innovation, Privacy/Profit or Privacy/Security are false and outdated thinking. It is encouraging to see stated recognition that the processing of personal data can be a "win-win" positive sum game rather than a zero sum game from the privacy officer of an organization built around processing vast amounts of personal data. This statement reflects one of the seven foundational principles of Privacy by Design – " Full functionality".

The Facebook report emphasises the importance of transparency and "Safe by Design"

One of the first major themes the Facebook/Ctrl-Shift report confronts is the question of transparency and educating individuals about what is done with their data. Information Transparency is a necessary pre-condition that enables educated decision making, but depending on execution, what appears to be information transparency can be an overload of information that becomes a barrier to good decision making. The ethical principles and implications of information transparency can be quite complex, and the concept of information transparency itself is subject to misunderstanding at the interface of business and technology.[3] The Facebook/Ctrl-Shift report notes the concerns many contributors had regarding the challenges of balancing education and transparency, and the heavy cognitive load of becoming data literate enough to provide informed consent regarding one's personal data.

The report emphasises the need to enable learning and build user confidence, but notes the inadequacy of a notice and consent model. The concerns and values expressed in the Facebook/Ctrl-Shift report again reflect fundamental Privacy by Design principles. The report recognizes that a lack of transparency results in loss of trust, but also that an overload of information is also counterproductive. Contributors noted ideas such as a "multi-layered approach" to transparency and communications[4]. Privacy by Design and Privacy Engineering offer some possible amelioration of this dilemma. Engineering a process from the perspective that privacy is the default, and focusing on simplicity in design so that users may more easily understand the choices they make regarding their personal data will empower people who lack strong data literacy to make informed choices without overloading them

[2] *"Facebook and Ctrl-Shift. "A New Paradigm for Personal Data: Five Shifts to Drive Trust and Growth". June 2016 https://www.dropbox.com/s/2mpczioqti3h47m/Report%203%20A%20new%20paradigm%20for%20personal%20data.pdf?dl=0 (accessed 31 July, 2016)*

[3] *Turilli, Matteo, and Luciano Floridi. "The Ethics of Information Transparency". Ethics and Information Technology. (2009). 11: 105-112*

[4] *Jacob Turowski, Facebook, Warsaw roundtable. "New Paradigm for Personal Data" p.7*

with too much information to understand the decision they make. Design choices like having a clear, consistent source for information and user settings that are not constantly changing, requiring people continually re-educate themselves on how to protect their data enable this value.

Focusing on the Individual: Individual control of one's own data

Another major theme in the Facebook report emphasizes the importance of re-centring an organization's approach to personal data on the individual's personal agency, empowering them to control their own data. The second "shift" in perspective calls for more choice and control than "passive consent", looking for a sustainable partnership in which the organization's goals and the individual's goals are aligned in a mutually beneficial partnership. As is stated in "A New Paradigm for Personal Data":

> *"What is more, when people have more control over their own data, more growth, innovation and value can be created than when they don't."*

This major theme again reflects the foundational Privacy by Design principle "Respect for user privacy". It also promotes ethical values, and notes that both process and outcomes must be fair. The contributors to the report noted the importance of clear communication in building trust in the relationship between a business and its customers.

Many of the ideas presented in the Facebook/Ctrl-Shift report are valuable and show an encouraging depth of thinking globally about the need to ensure that organizations and business models based on the processing of personal data consider the impacts on individuals and engage them as partners in a fair relationship, looking for a sustainable, "win-win" situation. Clear communication, transparency in processes, and encouraging the personal agency of the individual by ensuring they have control over their own data are ways to promote outcomes of an organization's process are aligned with customer expectations. The "paradigm shift" promoted in the report recognises that the false "trade-off" dichotomy of zero-sum game thinking may pit an organization against its customers in an antagonistic relationship that reduces trust. This type of relationship is likely to be unsustainable for long-term business benefit. It may also promote a framework for decision making that weighs towards unethical decisions and processes with adverse outcomes.

THE “NEW PARADIGM” IN ACTION

Facebook’s “News Feed Values” describes to its users the approach and priorities considered in algorithmically prioritizing content to populate their News Feed. One of its seven main value statements is *“You Control Your Experience”*, acknowledging that *“Ultimately, you know what's most meaningful to you”*. This introduction is used to explain the dual layer of user controls such as “unfollow”, “hide”, and “see first”, and incorporation of user behaviour or “feedback” into algorithmic decisions to show or hide content.[5]

The Adblock Arms Race

Facebook’s VP for Ads and Business Platform picked up on the idea of Individual Control in a blog post on changes to Facebooks platform regarding ads:

> *“*We’ve designed our ad formats, ad performance and controls to address the underlying reasons people have turned to ad blocking software. When we asked people about why they used ad blocking software, the primary reason we heard was to stop annoying, disruptive ads. As we offer people more powerful controls, we’ll also begin showing ads on Facebook desktop for people who currently use ad blocking software.*”*[6]

This is a technical engineering focused solution to problem rather than a holistic one that one that considers ethical ramifications or even cause and effect.

In the absence of the marketing industry’s respect for Do Not Track, users turned to Adblocker technology as a way to retain control over what content they choose to view. The need for such technology has been affirmed by the ability of adblockers to prevent malware-laden ads from infecting users’ computers. However putting aside the basic need to protect against malvertising attacks, adblocker technology may also be seen as the technological equivalent of turning the page as soon as you see that the content on that page is an advertisement. The reader recognizes that content is advertising which they do not wish to read and chooses not to read it; the adblocker does this by proxy, recognizing certain content that the user has signified it does not wish to read and hiding it from view.

As Facebook’s business model is dependent on advertising, it’s very important to them not just to ensure they can deliver advertising but to strike a balance that ensures it is effective. Ability to deliver advertising is a legitimate interest. However, it is also necessary to ensure that this method of advertising is sustainable, ethical, and lawful.

Does this comply with EU Data Protection rules?

There are two likely mechanisms by which Facebook’s announced bypassing of adblocker technology might be possible. The first has been seen in adblocker-blocking technology used by websites such as Forbes.com. This technique requires writing to and from the user’s device in order to detect whether a user’s browser has ad-blocking software installed.

[5] *https://newsfeed.fb.com/values/*

[6] *Bosworth, Andrew. http://newsroom.fb.com/news/2016/08/a-new-way-to-control-the-ads-you-see-on-facebook-and-an-update-on-ad-blocking/*

Essentially, this falls under the EU legislative description of "cookies" and is unlawful under the ePrivacy Directive (2002/58/EC). Under this Directive on privacy and electronic communications:

> *Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms.*

While the ePrivacy Directive recognizes that tools like "cookies" (and other methods of reading from and writing to individual's computers or smartphones) can be legitimate and useful, the ePrivacy directive stipulates that they should be allowed only for legitimate purposes, and "*with the knowledge of the users concerned*" because these tools can be incredibly invasive. By their nature, they:

> *. . . gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.*

This directive is transposed into Irish Law in section 5 of SI 336 of 2011, which stipulates that:

> *(3) A person shall not use an electronic communications network to store information, or to gain access to information already stored in the terminal equipment of a subscriber or user, unless*
> *(a) the subscriber or user has given his or her consent to that use, and*
> *(b) the subscriber or user has been provided with clear and comprehensive information in*
> *accordance with the Data Protection Acts which—*
> *(i) is both prominently displayed and easily accessible, and*
> *(ii) includes, without limitation, the purposes of the processing of the information.*

This is the legislative framework under which Facebook Ireland (which governs the processing of personal data of Facebook's EU customers) stands. Adblocker-blocking technology by its nature writes from and reads to information stored in the terminal equipment of a user without their prior knowledge or consent. As such, adblocker-blocking technology does not comply with either Irish law or overarching EU legislation, and is likely not in compliance with the legislation of other EU countries. The General Data Protection Regulation brings with it a stricter definition of consent and also a broader definition of what constitutes personal data, with a description that clearly includes browser fingerprinting as well. A revised and updated ePrivacy directive will be consistent with the GDPR, and it is highly unlikely that under these conditions adblocker-blocking technology will be considered lawful under new regulations. If Facebook's announced ability to bypass ads is in fact using an adblocker-blocking technology, it is likely to be in breach of European Data Protection laws, which uphold the societal ethical values that privacy and the protection of personal data are fundamental human rights that should not be violated.

Advertorial Content and Advertising standards

However, Facebook's announcement may suggest they are taking a different tack. Facebook hosts advertising content natively rather than employing third party advertisers. At a basic level, advertisers have the option of placing ads in either the right column (out of the regular eye line of users browsing their news feed, or in the News Feed itself as "sponsored" content:

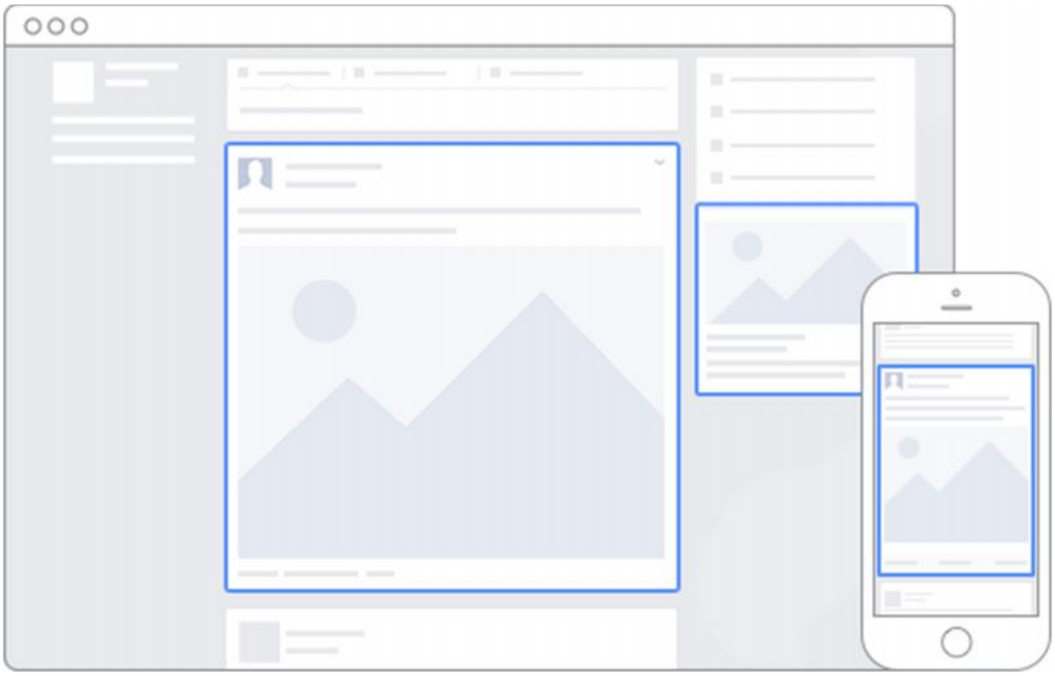


Figure 2: Facebook Guide to Advert Placement for Desktop and Mobile[7]

The question raised by Facebook's advertising, then, is when this becomes deceptive. Right column ads on Facebook's page are more clearly recognized as advertisements because of the page formats (and thus also more easily ignored by users), but advertising in the News Feed appears to be native content that could be seen as deceptive advertising. In the absence of (illegally by European Data Protection Law) writing to and reading from a person's computer without their consent to determine the presence of adblocker software, the other option to "defeat" adblockers is to make advertising content indistinguishable from other content, essentially disguising from a user the fact that content is advertising. If Facebook is to create News Feed advertisements that escape adblocking technology, it is likely that it would be formatted in a way that fits the definition of deceptive advertising practices by both US and European standards. Either they make a clear, transparent statement that the content is advertorial, or they risk falling afoul of legal and industry standards for deceptive advertising practices.

In the context of the United States, this sounds like it might well be Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices. An act or practice is deceptive where *"a representation, omission, or practice misleads or is likely to mislead the consumer"*. The FTC has made it very clear through its history of prosecution that the format of ads that

[7] *https://www.facebook.com/business/ads-guide?tab0=Mobile%20News%20Feed (Accessed 31 August, 2016)*

"*deceptively mimicked the format of news programming or otherwise misrepresented their source*" are indeed considered deceptive advertising:

> "*The FTC considers misleadingly formatted ads to be deceptive regardless of whether the underlying product claims that are conveyed to consumers are truthful*."[8]

Outside of the United States, Facebook is administered by Facebook Ireland. The Code of the Advertising Standards Authority for Ireland states the following:

> *3.31 A marketing communication should be designed and presented in such a way that it is clear that it is a marketing communication.* [9]

Advertisements on Facebook clearly fall under the scope of the ASAI Code, which includes:

> *2.2 (e) marketing communications carried on electronic storage materials and all other electronic media and computer systems; including but not limited to: online advertisements in paid-for space (including banner or pop-up advertisements and online video advertisements); paid-for search listings; preferential listings on price comparison sites; viral advertisements; in-game advertisements; commercial classified advertisements; advergames that feature in display advertisements; advertisements transmitted by Bluetooth; advertisements distributed through web widgets and online sales promotions and prize promotions;*
>
> *2.2 (h) marketing communications in non-paid for space online, under the control of the advertiser or their agent, including but not limited to advertisers' own websites.*

These ethical standards are backed up by legislation, as section 55(1)(q) of the Irish Consumer Protection Act of 2007 states that, among other practices, a trader shall not "*use editorial content in the media to promote a product (if a trader has paid for that promotion) if it is not made clear that the promotion is a paid promotion*".

While one might argue that this does not prohibit Facebook from algorithmically disguising the difference between sponsored content (ads) and user generated content or news, it does mean that any trader in Ireland and in other European countries purchasing advertising from Facebook would be violating the Consumer Protection Act 2007 or other broadly similar, robust, consumer protection laws. This may not be an ideal model for organizations that want to promote their services legally, let alone ethically.

Whether Facebook is actually violating European Data Protection laws or both European and American advertising standards for false advertising, what they are doing is producing a result that directly contradicts the standards they claim to espouse. If you strip away the magical thinking of the technology layer, what you have is in fact disguising content in order to force advertising content on people who have signaled that they do not want to see that

[8] *https://www.ftc.gov/tips-advice/business-center/guidance/native-advertising-guide-businesses*

[9] *Advertising Standards Authority for Ireland. Code of Standards for Advertising and Marketing Communications in Ireland http://www.asai.ie/wp-content/uploads/ASAI-CODE_2015_DEC15_Revision.pdf*

advertising content and taken steps to avoid seeing that content. Whether or not one agrees that this is ethical or legal, it is in conflict with the stated values communicated to Facebook's users.

One might argue that in agreeing to use Facebook's services users have consented to view the advertising that Facebook serves to them. However, this would be a difficult argument to make under EU legislation's requirement for specific, affirmative consent. It also subverts the emphasis on user control, and user education in Facebook's own messaging and in the Facebook/Ctrl-Shift report, "A New Paradigm for Personal Data". The reliance on up-front blanket consent raises an even larger ethical issue in one of Facebook's newest products.

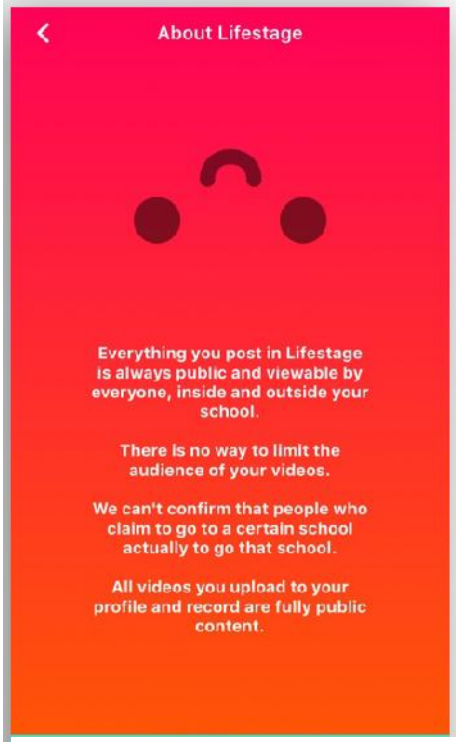
Lifestage

Lifestage, a newly released Facebook product, continues this pattern of subverting the values of Privacy by Design. In "A New Paradigm for Personal Data" Facebook and Ctrl-Shift highlight the problem of focusing on Education and consent-based models for data sharing, as the competing demands on people's attention and ability to filter information means that expecting individuals to be able to navigate complexities and make educated, data literate decisions to ensure their data is protected puts an undue burden on the public that is not seen in other sectors such as food safety. Among other things, this is essentially an argument for privacy by design and privacy by default, although the report uses the terminology "Safe by Default".

Facebook's newest app, Lifestage, is targeted specifically to children and teens, requiring connection to a school. (While the app states its target audience is High School age students, it has been noted that the graphic design of the app would appeal more to younger children, likely to be considered "immature" looking by high schoolers.) Lifestage seems to be a response to the fact that people are no longer sharing new and personal content on Facebook, attempting to recapture the youth market and the "old-school" profile curation of Facebook circa 2004. Nineteen-year-old product developer Michael Sayman describes how Lifestage works as "curating a public profile", by of adding videos to multiple profile fields.

Creating and curating a public profile, How It Works:

- *Build a profile by adding videos to fields of the things you like, the things you don't, how you do things, and more…*
- *Discover others who are into the same things you are into and connect with them.*
- *Share to dozens of fields in various sections of your profile such as "Music", "Home", and "School".*
- *Change out and replace your videos in fields at any moment, as often as you like.* [10]



About Lifestage

Everything you post in Lifestage is always public and viewable by everyone, inside and outside your school.

There is no way to limit the audience of your videos.

We can't confirm that people who claim to go to a certain school actually to go that school.

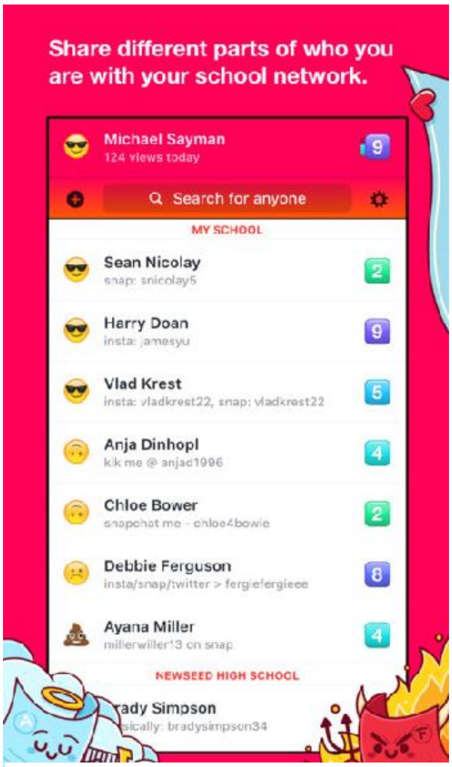
All videos you upload to your profile and record are fully public content.

Figure 3: Lifestage App Sign up process privacy statement

Unlike Snapchat, which this app appears to have been developed as direct completion, Lifestage videos do not disappear after 24 hours.

All data posted in Lifestage is public, with a one-time warning in the set-up process. The app lacks valid controls on whether or not users who have signed up are of the age they stated or whether they go to the school they claim. This is in fact less secure than early Facebook, which at the very least required College and University students to have a valid .edu email address from the universities connected to Facebook.

The app incentivizes users to give as much information as possible, publicly quantifying how often user's profiles have been viewed and publicly assigning different status emojis to users who have completed lots of fields and frequently update their field. This incentivizing is constructed in context of the social competitiveness of many teen social circles, suggesting that social validation would become paired with public and irrevocable sharing of one's data.



Share different parts of who you are with your school network.

Michael Sayman
124 views today
9

Search for anyone

MY SCHOOL

Sean Nicolay
snap: snicolay5
2

Herry Doan
insta: jamesyu
9

Vlad Krest
insta: vladkrest22, snap: vladkrest22
5

Anja Dinhopl
kik me @ anjad1996
4

Chloe Bower
snapchat me - chloe4bowie
2

Debbie Ferguson
insta/snap/twitter > fergiefergieee
8

Ayana Miller
millerwiller13 on snap
4

NEWSEED HIGH SCHOOL

rady Simpson
sically: bradysimpson34

Figure 4: Lifestage App Example Screencap

As Lifestage is targeted targeted at teens, middle and high-schoolers, barring access to users over 21, the app specifically targets people who are below the age of consent, below the age where they are considered competent to make legal decisions or sign contracts. This makes it particularly troubling that users are given a single point of consent when downloading the app, informing them that all their information will be publicly visible. The app only allows users between the ages of 13-21, avoiding a requirement for parental consent under COPPA. However, this design does not consider varying ages for required parental consent in other legal frameworks. Under GDPR, unless EU countries specifically introduce legislation lowering

[10] https://www.facebook.com/ms/posts/1102799113148105

the age at which parent or guardian consent for processing personal data, parental consent for the processing of children is required up to the age of 16 years.

The lack of choice regarding privacy settings certainly "simplifies options", but the single option of having everything public or not participating in a social activity raises several troubling ethical implications regarding the gamified incentivization to make public personal data, targeted to a population whose brain development is ongoing and who are also a frequent target for bullying and victimization. (The inability to keep personal information private does nothing to mitigate bullying.) Journalists have already raised questions regarding the security implications of the app, showing that Lifestages "makes it shockingly easy to stalk high schoolers"[11]

Full consideration of possible ethical and safety implications of a new app are not something that one would necessarily expect a 19-year-old prodigy whose previous apps had not focused on processing personal data to have immediately grasped, but an organization with proper governance should have a review process which might flag information risks and guide project managers in considering the implications of data processing. If an organization is to promote "Safety by default" as a value, as is suggested in the Facebook/Ctrl-Shift report, it must provide organizational support for responsible and ethical practices that consider information, privacy, and security risks.

WhatsApp

In 2014, Facebook acquired the popular OTT messaging service WhatsApp, promising WhatsApp's users that WhatsApp's privacy policies and practices would not change under Facebook's ownership, and stating that WhatsApp and Facebook would remain separate. At the time of sale, WhatsApp founder Jan Koum discussed his childhood in the USSR as a background for his reassurances that WhatsApp valued its users' privacy and would continue to operate independently under Facebook to preserve the value of "knowing as little about you as possible". Koum expressed deep personal understanding of the chilling effects of surveillance on people's behaviour and communication patterns:

> *One of my strongest memories from that time is a phrase I'd frequently hear when my mother was talking on the phone: "This is not a phone conversation; I'll tell you in person." The fact that we couldn't speak freely without the fear that our communications would be monitored by KGB is in part why we moved to the United States when I was a teenager.*[12]

Although WhatsApp was not the most secure messaging service on the market, under Facebook's ownership it had been hailed for a major step forward on an ethical stance towards privacy in introducing end to end encryption to its messaging services. "Our fundamental values and beliefs will not change. Our principles will not change."

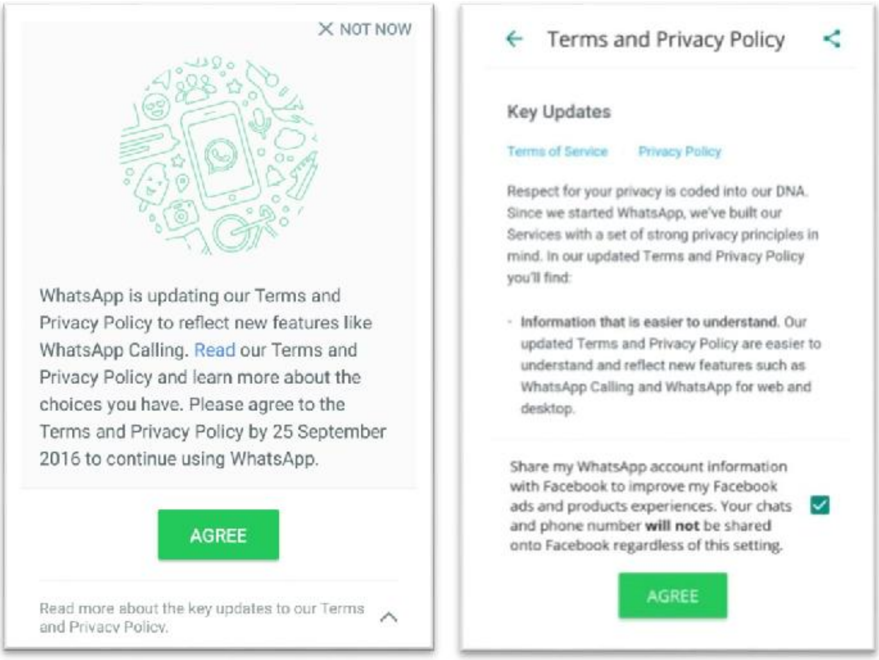
The August 25, 2016, WhatsApp announced changes to its privacy policies that are being criticized as a "betrayal" of the values and principles WhatsApp had previously espoused.

[11] *Ian Karr and Mike Murphy, "Facebook's newest app makes it shockingly easy to stalk high schoolers" Quartz. http://qz.com/764562/facebooks-newest-app-makes-it-shockingly-easy-to-stalk-high-schoolers/ (Accessed 31 August, 2016) See also: https://www.fastcodesign.com/3063083/facebooks-new-teen-app-freaks-me-out-and-im-only-23*

[12] *https://blog.whatsapp.com/529/Setting-the-record-straight (Accessed 31 August, 2016)*

One aspect of this change that critics found particularly disturbing was the seemingly underhanded way the announcement of the change and how consent was acquired. App users were given an announcement regarding the changes to the Terms and Privacy Policy describing a focus on "new features" with a large agree button. Only upon clicking "Read more about the key updates" were they presented with a pre-ticked box consenting to

> *"Share WhatsApp account information with Facebook to improve my Facebook ads and products experiences".*



WhatsApp is updating our Terms and Privacy Policy to reflect new features like WhatsApp Calling. Read our Terms and Privacy Policy and learn more about the choices you have. Please agree to the Terms and Privacy Policy by 25 September 2016 to continue using WhatsApp.

Read more about the key updates to our Terms and Privacy Policy.

Key Updates

Respect for your privacy is coded into our DNA. Since we started WhatsApp, we've built our Services with a set of strong privacy principles in mind. In our updated Terms and Privacy Policy you'll find:

- **Information that is easier to understand.** Our updated Terms and Privacy Policy are easier to understand and reflect new features such as WhatsApp Calling and WhatsApp for web and desktop.

Share my WhatsApp account information with Facebook to improve my Facebook ads and products experiences. Your chats and phone number **will not** be shared onto Facebook regardless of this setting. ☑

Figure 5: WhatsApp Policy Change Announcement and Consenting. Note: the pre-ticked box consenting to share account information with Facebook is only visible upon following the link at the bottom of the first page to "Read more about the key updates to our Terms and Privacy Policy"

The design of the announcement and consenting here is designed in a manner that will likely result in uninformed– and indeed invalid—consent to process personal data. The user experience is confusing. Users have reported clicking large green "Agree" button without even seeing there was an option to read more about what they were agreeing to. Pre-ticked "consent" boxes are in breach of EU Consumer Rights and Data Protection legislation ensuring that individuals are not tricked into inadvertently consenting to processes or agreements they would not have willingly consented to.[13] A hidden pre-ticked box only visible through a link that does not inform the reader that there is a choice to be made is highly unlikely to pass muster as valid consent. The user experience resulting from the process design here is an outcome that contrasts strongly with the stated values of the company that is likely to result in a loss of trust. Additionally, trust is likely to be lost if users feel tricked into an agreement they did not know they were making.

The resulting outcomes of the data sharing process also risk adverse ethical impacts. The new updated privacy policy has changed so that user data may be shared between Facebook

[13] *Directive 2011/83/EU of 25 October 2011 and the Article 29 Working Party Opinion 15/2011 both state that pre-ticked boxes do not constitute valid consent.*

and WhatsApp. Aside from the actual content of the messages which are still encrypted end-to-end, WhatsApp user data will be shared with Facebook and other Facebook-owned companies:

> *Facebook and the other companies in the Facebook family also may use information from us to improve your experiences within their services such as making product suggestions (for example, of friends or connections, or of interesting content) and showing relevant offers and ads.*

While the internal content of WhatsApp messages may be kept private and not shared with other Facebook services, the contacts and other metadata that are shared run the risk of exposing sensitive personal data in ways that Facebook and WhatsApp have not designed for. While the intent of processing may not be unethical, a failure to design processes taking into account the risks of adverse impact can result in ethical failure and violation of individuals' rights. This kind of inadvertent damage has already been seen in the combining of mobile phone numbers with other Facebook user data resulting in breach of privacy regarding sensitive personal information.

Recently a psychiatrist noticed that while she rarely used Facebook and shared very little data with the service and had not "friended" any of her clients, the "People You May Know" feature was highlighting many of her clients for friend recommendations. Even further, she found out that Facebook was recommending her patients to each other as friends. Facebook has not responded with a clear explanation of exactly how this breach of individuals' sensitive personal data may have happened. After a similar situation in which Facebook recommended as friends two people whose only contact had been attending the same gathering as parents of suicidal teens.[14] These situations highlight how a process design that does not take into account the risk of adverse effects on privacy and other ethical implications can result in inadvertently outing people in extremely sensitive situations without their consent.

Ironically, the main stated reason for sharing this data, "improving your ads on Facebook" may be counterproductive, as users tend to find personally targeted ads "creepy". In fact, Proctor and Gamble have recently decided to move away from targeted Facebook advertising, as they are finding advertising with a broader reach more effective than personalized targeting.[15]

[14] Hill, Kashmir. http://fusion.net/story/339018/facebook-psychiatrist-privacy-problems/ See also: Kashmir Hill. "Facebook is using your phone's location to suggest new friends—which could be a privacy disaster" http://fusion.net/story/319712/facebook-now-says-phone-location-not-used-to-recommend-friends / (Accessed 31 August 2016)

[15] *http://www.wsj.com/articles/p-g-to-scale-back-targeted-facebook-ads-1470760949 (Accesssed 31 August, 2016*

CONCLUSION

To be fair, the introduction of the Facebook report concludes:

> "Our goal is to portray the key issues facing participants within the data driven economy, rather than focus on any individual company or actor. Therefore readers should note that the paper does not necessarily reflect the views of its commissioner, Facebook, and should not be interpreted as stating any specific intent on their part."

We do not consider this disclaimer fully relevant, as the language described in the report is consistently reflected in Facebooks official communications to its users. This language, consistently phrased in a manner that espouses value for privacy, promotes individual autonomy, and argues for a positive sum game, is being used in conjunction with actions that subvert many if not all of the principles espoused.

The messaging between Facebook's Privacy Officer's statements, the report "A New Paradigm for Personal Data", and Facebook's user guide pages tend to be consistent. However the outcomes of the organization's actions do not match the expectations engendered by this message. This disconnect is likely to result in individuals' distrust of the organization and attempts to regain a sense of lost control over individuals' data, whether this is through reduced use of the service, reduced sharing of personal data through the service, attempts to subvert perceived invasiveness through privacy-enhancing tools or deliberately seeding false data, or abandoning the organizations services for competitors. If an organization desires for individuals to continue trusting it with their personal data, it must not only promote values that engender trust, a "sustainable personal data ecosystem", it must also ensure that the outcomes of its products and processes match the expectations that it will behave in congruence with these values. If it promotes "individuals' control of their own data", it must design and execute processes in a way that actually give individuals control of their data rather than "ethics-washing" its promotional material while violating individual autonomy and invalidating choice. Intent is made clear in the ethical choices made in action. Engineering an override of the stated preferences of individuals is incompatible with ideals of centring the individual Essentially rolling back on the distinction between advertising and content—such as news—violates ethical standards of transparency, and likely advertising standards in multiple countries.

However, we cannot ignore the role of the individual in policing the ethical conduct of companies whose products and services they use. Nor can we discount the need for effective, independent Regulators to support individuals in that task.