This Message Will Self-Destruct: The Growing Role of Obscurity and Self-Destructing Data in Digital Communication

by Christopher Kotfila

Practical obscurity is a legal term introduced in 1989 by the Supreme Court in the U.S. Department of Justice v. Reporters Committee case [1]. This decision created a legal precedent for the idea that some information, despite being made public in a specific place or at a specific time, is for all practical purposes private (or “obscure”). The court ruled that because the cost associated with obtaining certain information was so high there was a reasonable expectation of privacy on the part of the subject of that information [2] and that the Department of Justice could not be compelled under the federal Freedom of Information Act to divulge information that it had compiled from otherwise publicly available records. While no single piece of information under the FOIA request was private, the aggregate collection of such obscure information was considered so costly as to imply a certain level of privacy. Obscurity in this somewhat technical sense gives us an interesting theoretical framework for understanding the frontier between private and public information in an era when aggregation has become a dominating force in the information marketplace. By refining the traditional public/private dichotomy through an understanding of individuals’ desire for this kind of obscurity, information policy advocates can better understand the complex set of factors that inform the expectations of their constituents.

The emergence of a new trend in social networking and communication – self-destructing data – sets the stage for obscurity to return to the information marketplace in force and signals a growing awareness of the public eye in modern social networking communication. Snapchat, Wickr and iDelete are all mobile communication applications that have emerged in the last several years for sharing images, videos and text messages among social networks of friends and colleagues. In many ways the base communicative activities
that these applications enable are no different from the standard activities mobile technologies have been providing for well over a decade. However, unlike iChat and other vendor-specific, real-time data sharing and communication tools, the new genre of messaging applications allows the sender to set an expiration date on the data being shared. Images and text messages literally self-destruct and can no longer be viewed by the receiver. Extending the definition of obscurity beyond the Supreme Court decision gives us a chance to see how time-bound “forgettable” information plays a vital role in communication and how a market is developing in modern technical communication circles to reclaim the element of obscurity that was once a constant but unseen aspect of our every day behavior and interactions.

A History of Obscurity

The term practical obscurity first occurs as a matter of jurisprudence in the 1989 Supreme Court decision cited above. At that time, journalists requested under the Freedom of Information Act the rap sheets of four brothers who had allegedly obtained defense contracts from an improper arrangement with a corrupt congressman. The FBI refused to release the rap sheets and the journalists sued, limiting the request to publicly available information. The case progressed through the district courts and was finally accepted by the Supreme Court in order to resolve the issue of whether releasing the documents was an unwarranted invasion of privacy despite the requested information having at one point been a matter of public record. The decision affected a number of different aspects of how agencies attempt to balance privacy and access when considering FOIA requests [2], but the most germane to the present conversation is the introduction of the concept of obscurity. The court ruled that, despite the rap sheet information having been public at one point, the cost to identify, locate and access that information created a reasonable expectation of privacy on the part of the brothers. In short, the court ruled that the rap sheet information was not simply public because it had once been public, but that a reasonable expectation of privacy existed because of the “practical obscurity” of the documents. Little jurisprudence has been based on the notion of practical obscurity as described by the Supreme Court in the Reporters Committee case, but a vibrant community of scholarship and discussion has emerged around the policy implications of obscurity in the digital age. (See [3, 4, 5, 6] for more resources.)

Evolution of Obscurity

Conversation as a mode of communication has traditionally included a kind of practical obscurity. Individuals must rely on memory if they wish to relay information beyond the initial interaction between two people. This memory of the information contained within the conversation becomes co-mingled with our own impressions and makes oral communication a highly noisy channel for communication. The childhood game of telephone provides ample evidence for why secondhand accounts of conversations are inadmissible in court. One may choose to believe rumors and gossip but there is a social understanding that spoken information is ephemeral, and, once communicated, up for interpretation on the part of the hearer. Information in this modality becomes almost instantly obscure, and it can be very difficult to hold the speaker responsible for the content of his or her communication.

Written documents as well as video and sound recordings resolve the issue of this kind of hearsay by fixing the data or message in some physical form. This fixity provides individuals in the communication chain a great advantage; they no longer have to rely on memory in order to transmit information from one individual to another. This advantage, however, comes at a price. Once it is fixed in a tangible physical form, authors of works can be held responsible for the information contained within them. Anything that is written down or recorded runs the danger of becoming public. By fixing it in a tangible form (whether analog or digital) the author trades a degree of control over his or her ideas for the ability to consistently communicate those ideas to others.

Information given physical form ultimately faces destruction and so one way or another passes into memory and is eventually either forgotten or incorporated into a larger social identity. To counteract the passage of time and the limits physical documents place on information access, copies of documents may be made in order to preserve or more widely distribute the information contained within them. Copies of physical documents are usually
Information retrieval technologies have allowed us to arrange and rearrange access to a dizzying set of public records and personal information.

There is a real cost associated with creating copies of a physical document and less valuable or highly specialized documents frequently remain scarce. Bestselling books, for example, may sell millions of physical copies while a government report on water quality may only be reproduced a few hundred times. The cost of copying creates scarcity, and this scarcity in turn creates a barrier to accessing the information contained within those physical documents.

The difficulty in locating certain documents means that even though they may be public or may have been public, they are currently “practically obscure.” This concept of obscurity challenges the traditional notion of information as either private or public. Instead of a binary model the obscurity of physical documents creates a nuanced spectrum of privacy based on the investment an individual is willing to make to acquire certain information.

Modern digital technology has made this kind of obscurity in many ways obsolete. Information retrieval technologies have allowed us to arrange and rearrange access to a dizzying set of public records and personal information. These technologies allow a well defined information need to quickly and efficiently cull away documents that are not relevant to an inquiring individual. This ability has had the effect of flattening the information landscape and bringing a growing corpus of publicly published information into focus. In the Reporters Committee decision the Supreme Court argued that despite information being made public at a certain place and time there were substantial privacy interests that could, and should, be protected by the difficulty of accessing and compiling that information [2].

Information retrieval systems have made it so that information once published is effectively place-less and timeless. What would have once been transient information has become a matter of fixed public record. Not a record stored in a dusty filing cabinet out of sight and out of mind, but a record in full public view, accessible by any inquiring individual regardless of motive. While many benefits have come from the power of relevance-based search engines, one of the costs has been a loss of obscurity – at least until the recent emergence of self-destructing data.

Obscurity Fights Back

Technologies that enable self-destructing data are increasingly penetrating the technology marketplace. Several emerging applications rely on data self-destruct mechanisms as the key innovative component to an otherwise mainstream technology. These companies have identified and tapped into consumer desire to create disposable, short-term information and are slowly but surely re-introducing obscurity into an otherwise flat and persistent information landscape.

Snapchat allows users to send images and captions to either a single friend or multiple friends with a time limit of between one and 10 seconds before the image or “snap” is no longer accessible. Self-describing as a “new way to share moments with friends” [7], Snapchat has become wildly popular since its launch in September of 2011 with co-creator and CEO Evan Spiegel claiming the service processes 150 million photos daily.

Snapchat unfortunately cannot assure that users who receive these snapshots do not use the phone’s built-in screen-capturing capabilities to save these images; it does however notify the sender when the receiver has screened captured the snap. In any case a determined individual with a camera can always take a picture of the phone, thus thwarting the intended use of the application. Snapchat is upfront about these vulnerabilities on its website [7]. Despite these limitations users have flocked to the service because of a perceived sense of the time-bound nature of the data that they share.

Snapchat places a strong emphasis on privacy, safety and digital citizenship [8]. Snapchat describes its own popularity in terms of the privacy...
it provides its users. What it is really offering is a way to thwart the permanent nature of digital information by allowing it to fade almost immediately into obscurity. This service is particularly interesting for increasingly information-aware individuals who want to share information in a personal context that might reflect poorly on them in other, less casual contexts.

Wickr, unlike Snapchat, focuses its branding and business model specifically on the security aspects of self-destructing messages and images. Wickr allows users to text, send images, videos and pdfs to individuals or groups and time limit access to those communications [9]. Wickr allows the sender to set the self-destruct time from between one second and five days and unlike Snapchat uses powerful military-grade encryption to prevent the servers that store and transmit those messages or images from identifying the sender or using the data for behavioral advertising or tracking. Additionally, Wickr uses forensic deletion techniques to ensure that messages and other media are irrecoverable once they have self-destructed. Finally Wickr makes a firm commitment to data privacy and transparency in its privacy policy: “You own your data. We do not share or sell any data about our users. Period.” [10]

While Snapchat seeks to appeal to users who want to “share a moment,” Wickr appeals to individuals who are deeply invested in the privacy of their communications. Wickr was created in June 2012 by a group of security experts and privacy advocates lead by Nico Sell, one of the organizers of the famous Def Con hacker conference. Sell’s vision is to bring the Wickr protocol to as many forms of online communication as possible. Using a patent-pending technology, Sell hopes to allow users to interact with any social network using Wickr to protect and time-bind the data and information placed on that network [11]. Wickr of course faces the same screen capture vulnerabilities as Snapchat. Unlike Snapchat, information on Wickr’s website does not directly address these vulnerabilities. With Wickr, self-destruction of messages and data is seen as a key component of a larger privacy strategy.

iDelete is a relatively new contender in the data self-destruction market. iDelete’s app looks to fill the same space as Snapchat but brings new value to market by blurring images and texts unless the receiver holds down on the screen [12]. iDelete claims this effectively disallows users from taking screen shots of images or texts; providing an additional layer of privacy. Released in March of 2013 the service suffers from some technical issues [13] but stands to bring a competitive advantage to the self-destructing data marketplace by combining several of the security features of Wickr with the ease of use of Snapchat and the added security of preventing screen captures [14]. iDelete is particularly interesting in the context of obscurity because it actually physically obscures the data, attempting to implement a communication mechanism that can only be read by another person. Because the message self-destructs, the information is transferred in a functionally similar method to oral communication. After a brief period, the only trace of the communication is in the minds of the sender and the receiver.

A Policy of Obscuring

The ability to have private conversations outside the observations of other humans and, increasingly, away from the behavioral profiling of automated processes is a vital aspect of a vibrant creative society. The ability to have private conversations outside the observations of other humans and, increasingly, away from the behavioral profiling of automated processes is a vital aspect of a vibrant creative society. One can argue that the timeless, eternally present, nature of information in the digital age represents a fundamental shift in the nature of human interaction. The willingness of individuals to publicly publish vast quantities of personal data has certainly had a dramatic effect on nearly every aspect of the social experience. Privacy advocates have frequently petitioned policy makers to ensure the populace is protected from its own impulses to over-share personal information. These advocates often argue that consumers are being taken advantage of by a technological elite due to a lack of education about behavioral tracking and profiling. Policy makers have in turn been hesitant to regulate in favor of protecting personal information in the online arena, fearing that such legislation would injure the growth of an industry whose
economic model is based on access to, and aggregation of, the very information privacy advocates would seek to protect.

The open market, an increasingly well-educated consumer base and the potentially disruptive technologies of self-destructing information enabled by applications like Snapchat, Wickr and iDelete are stepping into this web of interests and stakeholders. The great strength of digital technologies is their ability to lower the cost of accessing information by making the cost of copying that information negligible. This irrevocably destroys the delicate ecosystem of privacy expectations that the obscurity of physical documents once protected. Self-destructing data is a deliberate countermeasure to this shift in the communication landscape and provides a way to reclaim control over the persistent nature of digital communications without having to artificially implement information policies that protect users or regulate content providers.

Resources Mentioned in the Article

[12] iDelete | Facebook: https://www.facebook.com/iDeleteAPP