YESHIVAT HAR ETZION

ISRAEL KOSCHITZKY VIRTUAL BEIT MIDRASH (VBM)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Halakha in the Age of Social Media**

**Rav Jonathan Ziring**

**Shiur #25:**

**The Unique Challenges of the Digital Age**

**Part II**

**Stealing Information**

We noted [last week](https://www.etzion.org.il/en/shiur-24-unique-challenges-digital-age-transfer-information-no-audience) that several authorities entertain the possibility that using information without permission may be a form of stealing — either due to an expanded understanding of *geneivat daat,* which usually refers to deception, but literally means the stealing of knowledge; or under the rubric of *she’eila she-lo mi-da’at.*

It is worth noting that certain Poskim specifically entertain this model when the question at hand is the stealing of trade secrets. Professor Nahum Rackover *(Ha-hagana al Tzinat Ha-perat,* Chapter Five*)* notes that that the *Kesef Kedoshim* (*CM* 183:4) refers to this astheft, as does Rav Shemuel Wosner (*Responsa Shevet Ha-Levi* 4:220). It is unclear to me whether this classification entails an acceptance of the notion of intellectual property in Halakha as real property, or they are using theft in the sense of *geneivat da’at* or loosely. What is clear is that when information is taken in such a way that it causes real monetary damage, these Poskim either fully or nearly equate the illicit use of it with theft.

However, it seems to me that even the use of information which would prevent people from being approved for loans (to use the example we mentioned in the previous *shiur*) would rise to this level. These Poskim seem to be motivated by their conviction that trade secrets have positive monetary value, not just that sharing them causes monetary harm.

**Consent**

One potential argument for why this discussion is irrelevant is that in most cases, the people whose information is being taken have given consent. In a case in which the information is obtained without consent (or perhaps, as in the Cambridge Analytica case, information was gathered from the Facebook friends of people who took a survey), then all the potential prohibitions discussed would apply. However, in a case in which users know that the price of accessing Google or Facebook is that their information will be used, shouldn’t that implied consent be enough to negate any potential prohibitions? This is even more true for applications that require one to provide consent that one’s information be shared before downloading the application.

The problem, already noted in secular literature, is that this consent is usually not given with a full understanding of the consequences. Take, for example this lengthy quote from an article in *The Guardian*. In it, the author highlights several issues we have discussed: that the information being gathered has real monetary value and has been commoditized; that the gathering of this information has not been treated as theft, but re-evaluating that assessment may be critical in developing proper ways of controlling it; and that while consent is often given, that consent may not be meaningful for a host of reasons:

Contrary to the oft-repeated rhetoric, data does not exist independently in the world, nor is it generated spontaneously. Data is constructed by people, from people. As digital studies scholar Karen Gregory puts it: “Big data, like Soylent Green, is made of people.” Wringing the value from data requires more than just collecting it. Gathering it requires expertise in creating, extracting, refining and using it. This often goes hand-in-hand with increasingly invasive systems for probing, monitoring and tracking people.

Now here’s the rub: if corporations and governments are going to up the ante by treating data as an asset, then we — the targets of this data imperative — should respond in kind. Many common practices of data collection should actually be treated as a form of theft that I call data appropriation — which means capturing data from people without consent and compensation.

People often do not even know how their data is taken and used, let alone how to give meaningful consent. Data brokers, for instance, aim to provide their services from the shadows, while amassing billions and trillions of data points about people worldwide.

Data-driven policing technologies are shielded by trade secrets, which prevent the public from knowing what data the analytics crunch and how it influences police activity.

When companies do seek consent, it is typically through terms of service agreements — overly long contracts are full of dense legal language that users are expected to “agree” to without understanding. It is a remarkable victory for the data appropriators that acquiescence has become the standard model for obtaining “consent.”

Data appropriation is a form of exploitation because companies use data to create value without providing people with comparable compensation. While some might argue that Google and Facebook pay us for our data with “free” services, this still does not account for the multitude of data appropriators that have no intention to provide some kind of mutual benefit to those whose data they possess.

The data as an asset paradigm has helped create a lucrative market for data — the data broker industry alone generates around $200bn in annual revenue — which cuts out the people that data is about.

In short, rampant practices of data appropriation allow corporations and governments to build their wealth and power, without the headache of obtaining consent and providing compensation for the resource they desire.

Data appropriation is surely an ethical issue. But by framing it as theft, we can lay the groundwork for policies that also make it a legal issue. We need new models of data ownership and protection that reflect the role information has in society.

In the Gilded Age 2.0, a laissez-faire attitude toward data has encouraged a new class of robber barons to arise. Rather than allow them to unscrupulously take, trade and hoard our data, we must reclaim their ill-gotten gains and rein in the data imperative.[[1]](#footnote-1)

What does Halakha have to say about this? There are many relevant sources on this issue, but we will explore a few, starting with the question of whether explicit agreement to terms one may or may not understand is acceptable in Halakha.

In general, the assumption is that one is bound by whatever one agrees to when signing a contract, regardless of understanding what is at stake. For example, *Shulchan Arukh* (*CM* 45:3) writes explicitly that even if one does not understand what one signs, one is bound by the contract.

Similarly, the Rema(*EH* 66:13) rules that a husband is bound by the terms of a *ketuba,* and he cannot avoid paying by claiming he was ignorant when he signed the *ketuba* and did not understand its implications.

The Rashba (*Responsa* 1:629) cites two opinions on the topic. His argument, accepted by the *Beit Yosef (EH* 66), is that we must not accept such arguments as then all ignorant people could avoid any obligations by claiming that they didn’t understand the details of the contracts they signed. (See also *Responsa Rashba* 5:228.)

Rav Ovadya Yosef assumes that this is the majority position (*Responsa Yabia Omer, EH* 3:13). The Rashba in that responsum seems not to rule in line with this position, but Rav Yosef assumes that this is only out of deference to Rav Meir (whose view we will discuss below), whom he cites as having already ruled otherwise.

In many of these sources, the assumption is that we simply do not believe the person claiming ignorance. However, the Sema (*CM* 45:5) cites a different passage from the Rashba (*Responsa Meyuchasot Le-Ramban* 77), arguing that the reason is more fundamental: when people sign a document, they rely on and trust the scribe. Thus, even if we know that they didn’t understand the terms, they are bound by them. The Shakh (*CM* 45:5) rules similarly.

One could have simply understood this as saying that people are responsible to understand what they are signing; and if they don’t, it is their fault. However, *Responsa Mahariaz Ansel* 49, cited in *Divrei Geonim* 102:20, argues that it is the trust for the scribe that is critical.

Rav Avraham Sherman (*Techumin* 8:163-165) contends that according to this formulation, only a contract reviewed by a trusted outsider would have this status, not a contract written by the opposing side (in his case, a bank was obligating someone based on a clause in the contract they had given him.)

However, as noted above, there are those who contest this. The Rashba (*Responsa* 1:629) cites the view of a Rav Meir, who argues that one may indeed claim not to have understood the implications of a contract one has signed and thereby be exempted from the obligations dictated therein. While the Rashba does not reverse the decision, most authorities assume that he disagrees.

However, certain authorities present a more nuanced position. For example, the *Knesset Ha-gedola* (commenting on *Beit Yosef, CM* 147:8) suggests that either 1) the Rashba would accept the argument that one did not understand a **detail** in a contract, but not that one did not understand the basic obligations one committed to; or 2) the Rashba would accept an argument for exemption if this a case of *anan sahadei,* a general acknowledgment that one did not understand. Rav Ovadya Yosef notes that some authorities, like Rav Betzalel Ashkenazi (*Responsa Rav Betzalel Ashkenazi* 24), cited by the *Knesset Ha-gedola* (*Beit Yosef, EH* 66)argue that one can only put forth such an argument when one has witnesses sign the contract. However, after signing a document oneself, one cannot make such an argument.

The relevance of these positions is clear when one does not read all the details in a contract made with a bank or the like. For many Poskim, this is never an excuse. Others, however, argue that if there is strong circumstantial evidence that one did not understand what one was agreeing to, or did not sign oneself and thus cannot be assumed to have understood everything, we would accept such a claim.[[2]](#footnote-2)

The upshot of these positions is as follows: according to most Poskim, one cannot claim not to have understood the implications of a contract one signed. Others maintain that this is a legitimate claim. Some will accept this only when there is strong circumstantial evidence that one did not understand the contract or had someone else sign.

Finally, based on the view of the *Knesset Ha-gedola,* there may be room to exempt someone from a detail found in the fine print, though not from the main obligations outlined in a contract.

So, does the fact that one accepts that one’s data will be used affect whether it can be used? An argument may be made that it does; after all, one is responsible to read the fine print. Either we assume that one should have read it, or we assume one actually did read it and understand it. On the other hand, when it is common knowledge that no one reads the full contract (and could not understand every detail in any case), an argument may be made that this cannot constitute full consent.

All these issues came to the fore when Mark Zuckerberg was questioned by the U.S. Congress about the way Facebook uses data and gets consent. Take, for example, this summary of that meeting from CNBC:[[3]](#footnote-3)

Republican Senator John Kennedy of Louisiana confronted Facebook CEO Mark Zuckerberg about the transparency of the social media company’s policies during a joint hearing of the Senate Judiciary and Commerce committees on Tuesday.

“Here’s what everyone’s been trying to tell you today — and I say it gently — your user agreement sucks,” Kennedy said. “The purpose of a user agreement is to cover Facebook’s rear end, not inform users of their rights.”

Zuckerberg appeared momentarily amused, but the comment hits at an issue central to Facebook’s data scandal: transparency. Critics argue Facebook users aren’t well-informed about Facebook’s plans for their data. Kennedy believed this partly because those plans are laid out in a long and complicated user agreement. Even Zuckerberg later admitted most users probably don’t read it.

“I would imagine probably most people do not read the whole thing,” Zuckerberg said. “But everyone has the opportunity to and consents to it.”

Just in case Zuckerberg wasn’t entirely clear on Kennedy’s point, the Senator left him with some colorful advice.

“I’m going to suggest you go home and rewrite it, and tell your $1,200-dollar-an-hour lawyer… you want it written in English, not Swahili, so the average American user can understand,” Kennedy said.

Zuckerberg presented the argument that all users have the opportunity to read the details; and if they don’t, that is their problem. Indeed, as Senator Kennedy noted, that might be enough to cover them legally, as it might be in Halakha. However, the point of the potential regulation, according to Kennedy, would be, in halakhic language, to accommodate the *Knesset Ha-gedola.* People need to actually understand the agreement, including the fine details.

Practically, this approach might lead us to distinguish between the data collection which people know about and have tacitly accepted, such as for targeted advertisements (which some people not only accept but prefer), on the one hand; and on the other hand, data collected for political purposes or (to use our example from last week) to determine who is approved for loans, which people do not realize and do not really accept.

However, this will be enough to cover only Facebook and other applications that require consent. When it comes to Google, for example, to whose terms no one ever explicitly consents, it may be that the information may be used with even less permission.

**Consent in *Hezeik Re’iya***

When dealing with Google, we are dealing not with explicit permission, but implicit permission. Perhaps we can gain insight as to the implications of this distinction if we return to our model of *hezeik re’iya.*

Concerning *hezeik re’iya,* the Gemara records a dispute as to whether one can acquire a *chazaka* to allow engaging in what would otherwise be *hezeik re’iya.* For example, if one has a window facing a neighbor in such a way that it violates the neighbor’s property rights and the neighbor does not protest, does that allow the person to continue having that window when the neighbor does protest?

**The Sages taught** in a *baraita*: There was **an incident involving a person who opened his windows into a courtyard belonging to partners and came before Rabbi Yishmael bar Rabbi Yosei,** who **said to him: You have established an acquired privilege, my son; you have established an acquired privilege,** and you may not be prevented from using the windows. **And he came before Rabbi Ḥiyya,** who **said** to him: **You toiled and opened** the windows; you must **toil and seal** them, as the partners have the right to prevent you from using these windows.

The Rishonim disagree as to whether this passage indicates that there is never a *chazaka* with regards to *hezeik re’iya,* and the neighbor may always claim that such a situation is harmful and force the homeowner to stop, or whether this case is unique. The Ri Migash (*Bava Batra* 2b) notes that the Rif rules that this passage indicates that there is never a *chazaka* in such a case, while the Ri Migash himself disagrees, arguing that one can establish a *chazaka.* However, in the above case, there is no *chazaka* for two reasons:

1. When neighbors are damaging each other, they can claim that their previous silence was not due to a lack of opposition, but due to the mutuality of the damage.
2. When neighbors damage each other in this way, it is not considered an action, as the windows have already been opened.

However, if someone does something active and no opposition is elicited, that would create a *chazaka.* The Rosh adds another distinction — a *chazaka* can be created by low-level *hezeik re’iya.* However, concerning open windows, a situation in which privacy may be utterly destroyed, one may always claim that this level of “damage” is unbearable.

Some Rishonim (Rashbam, Rabbeinu Gershom, Meiri to *Bava Batra* 59b) argue that even in the case of windows, the Gemara only means that there is no immediate *chazaka;* but after a requisite amount of time, there would be a *chazaka.*

The Ramban (*Chiddushei Ramban* 59b) explains the rationale for rejecting *chazaka* in cases of *hezeik re’iya.* The Gemara assumes earlier (23a) that for certain intensely harmful damage, one cannot develop a *chazaka,* as in such situations, not just property but people are harmed. *Hezeik re’iya* harms the people themselves because it causes *ayin ha-ra;* it enables *lishna bisha/ lashon ha-ra;* and it breaches *tzeniut,* privacy.

The majority position is to accept that a *chazaka* can be created as long as the potential damage was created in an active way that should have elicited a response (*Shulchan Arukh, CM* 154:7-8). However, the Rema notes (ibid. 7), based on the Rashba (*Responsa Ha-Rashba* 3:180, cited by *Beit Yosef* ad loc.) that even if such a *chazaka* may be established to leave a window open, a homeowner cannot violate a neighbor’s privacy by actually staring into the neighbor’s property.

Let us apply this principle to our case. Assuming that the use and sale of data (even stripped of identity markers) constitutes a potential violation of *hezeik re’iya*, as people learn about new implications to the use of their data, does the fact that they have not protested until now prevent them protesting at the present time?

On the one hand, once people learn about what Google can utilize their data for and they continue to use the service, one might argue that this is a new act of consent. What about the previously-collected data? May companies like Google simply assume they have consent because they have not received pushback? (Granted, the objections have been growing recently.)

According to the Ramban, one may argue that this type of invasion of privacy is so great that people can always demand that their data not be used, even the parts of it already collected. According to the Ri Migash, the situation is more complicated. One might argue that the fact that people don’t actually realize what is going on makes this case similar to the case of the jointly-owned courtyard, where the passivity with which people are damaged makes a lack of response not dispositive.

More importantly, according to the Rema, even if a *chazaka* can be established, this only allows leaving the window in place, parallel to allowing Google to collect data. However, to use the data in such a way that is considered a breach of privacy remains prohibited always.

I am unsure of the exact conclusions to derive from this, but I think the nuances raised by the Poskim in the context of *hezeik re’iya* may help us shape a language for determining what assumptions may be made about the type of data which it is legitimate to collect and utilize.

***To’elet***

It should be obvious that in cases of *pikuach nefesh,* in which data is used to prevent terrorist attacks or other dangerous criminal activity, it would be legitimate for the authorities to access information. However, when it comes to lower-level *to’elet,* we have previously discussed the possible differences between *lashon ha-ra* and breaching confidentiality. How we conceptualize the accessing of data may generate different conclusions. A friend pointed out to me that, theoretically, a bank could claim that there is *to’elet* in its knowing whom to lend to. While this may justify accessing this type of information if the only problem is *lashon ha-ra,* as we have noted, there are many other prohibitions in play which complicate the matter. More research must be done on these issues.

**Conclusion**

More than any of the other *shiurim* I have written, the previous two have convinced me that:

1. The challenges that we face in the digital age are in many ways unique.
2. Some of these challenges have not been dealt with by the Poskim at all.

In these *shiurim,* I have tried to present my thoughts, though I must note that they are tentative and meant to begin the discussion. My hope is that the Poskim will begin to grapple with these questions in serious ways and push the conversation forward.

1. “Companies are making money from our personal data — but at what cost?” by Jathan Sadowski, available at:

   https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon [↑](#footnote-ref-1)
2. See here for a summary of these issues: <https://shulchanaruchharav.com/halacha/is-a-signed-document-legally-binding-if-one-was-unaware-of-its-content/> [↑](#footnote-ref-2)
3. <https://www.cnbc.com/2018/04/10/senator-to-zuckerberg-your-user-agreement-sucks.html> [↑](#footnote-ref-3)