ISSN: 0975 – 5632

VICTORIAN JOURNAL OF ARTS

VOL. 10, ISSUE- I

JANUARY, 2017

VICTORIAL JOURNAL OF ARTS

ISSN: 0975 – 5632

Vol. 10, Issue-I January 2017

Publisher: Office of the Principal, A.B.N. Seal College, Cooch Behar

EDITORIAL

Publishing a bilingual multidisciplinary journal in Humanities has a few issues to resolve. First is the issue of linguistic hierarchy. In a particular Issue the English language articles may come first followed by the articles in Bengali language, or it may be the other way round. The order may then alternate over subsequent Issues. This way of tackling the problem leaves one question open: which is the language to start with? A clever answer is: we have flipped an unbiased coin. There can be another answer, and this takes us to the second important issue to resolve for the editors. It may be proclaimed that the order in which the two languages appear has been given no importance at all. The articles have instead been sequenced in such a way that the reader, supposedly conversant with both Bengali and English, can find articles in a cluster for any area of study. This is exactly what has been attempted here, and within each cluster, there is the coin to take care of the languages. There is, however, no impartial rule to sequence the clusters themselves, and, therefore, this job is best left to the predilections of the editors who, finding themselves unhinged from the rigour of rational ethics, may now indulge in little sins.

The current issue contains, like its predecessors, a wide range of contents cutting across Philosophy, Religion, History, Gender Studies, Literature, Economics, and Geography. The diversity of the articles is, however, not only in terms of contents and their temporal sweep but also in terms of the range of inscribed worldviews, which defies the unity that any authoritarian production of knowledge tries to enforce. This journal is an open forum where varied, often contesting, ideas and ideologies can not only cohabit but are also actively encouraged. This is not always done to find a synthesis, but to acknowledge that text is a site of battle fought by many readings, that no reading is final, that a new entry point of analysis is always a possibility, and tolerance to this possibility is what discourse asks from scholarship.

As the reader turns over the pages the lure of reading enchants. A survey of a sleepy, misty Himalayan village; a study in *avatars* in Hindu scriptures; religion as a collective mind vis-à-vis religion as a means of transcendence for the individual; Tagore's faith in religion as a deeply humanist project; a study of Val Plumwood's critique of androcentric logic; an anti-Freudian analysis of gender; role of Muslim women in India's struggle for independence; the dynamics of Sino-Indian relation; *Yakshapuri* in Tagore's *Rakta Karabi* as a microcosm of alienated urban life under capitalism; the subalterns in Bengali short stories; the pervading faith in God and afterlife in Shirshendu Mukhopadhyay's writings for children; a study in cinematic adaptation of literature…the list continues. This issue also contains an invited contribution from Udayan Roy from whom we have received a lucid book review on *phishing*. This review warns us that attacks from phishing predators may not always come from the internet, as commonly believed. The net (no pun intended) is much wider, and the folly is rooted in the ill-restrained market institution that plays on the desires of fools that so many consumers are.

Happy reading.

Debabrata Lahiri
Editor-in-Chief

CONTENTS

Predators and Prey

Udayan Roy[1]

Book Review

Phishing for Phools:The Economics of Manipulation and Deception **by George A. Akerlof and Robert J. Shiller, Princeton University Press, Princeton, New Jersey, USA, 2015**

Rational behavior is a key assumption in much of economic theory. When people are rational, market-based economies turn out to be efficient, in the sense that government intervention would not be able to help some people without hurting others. The rationality assumption has long been criticized. And lately, the emergence of behavioral economics has amplified the criticism. Now, George Akerlof and Robert Shiller are making the case that when not all people are equally rational, the same profit motive that economists celebrate loudly may become a cancer in the body economic, with those who are more rational devoting their energies to the exploitation of the mental vulnerabilities of the less-rational.

In a world of rational people, every voluntary exchange must be a win-win outcome; the seller and the buyer must both expect to benefit from the exchange, or else the exchange would not happen. Moreover, rational people strive to develop new ways to satisfy the genuine needs of other rational people, because that is the only way one can sell goods and services to others and thereby earn a living. In such a world, the profit motive is at its glorious best. It endows capitalism with both efficiency and dynamism.

Akerlof and Shiller are questioning this received wisdom and talking about the dark side of the profit motive. When some people are more rational than others, those who are more rational may end up focusing on the mental vulnerabilities of those who are less rational. Their innovative abilities may be channeled by the profit motive into developing cleverer and cleverer ways of exploiting the mental weaknesses of the less-rational.

This idea may not surprise non-economists. (After all, to take just one example, why, given our current scientific knowledge, would one person sell a cigarette to another person?) But Akerlof and Shiller are academic economists, and they are speaking out against the unwillingness of academic economists to systematically study the implications of the profit motive under conditions of varying levels of rationality across economic agents. They are trying to change the dominant discourse within their field.[2]

---

[1] Udayan Roy is Professor of Economics, Long Island University, Brookville, New York.

[2] Akerlof and Shiller have both won the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel; Akerlof in 2001 and Shiller in 2013.

We are used to the notion that ideas and objects can be used for good and for ill. Nuclear physics can be used to generate energy, and to make weapons of mass destruction. Chemistry can be used to make life-saving medications, and narcotic drugs and poisons. Guns are used for defense, and for offense. Food provides essential nutrition, and is also the source of disease. Betting can be both heedless gambling, and the sensible hedging of one's risks. Akerlof and Shiller are arguing that the profit motive is like-wise a two-edged sword. It has given us cornucopia. But it can also pit people against people in the economic realm.

An online dictionary defines *phishing* as the act of trying to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one. Akerlof and Shiller, however, are using the word in a broader sense:

> It is about getting people to do things that are in the interest of the phisherman, but not in the interest of the target. It is about angling, about dropping an artificial lure into the water and sitting and waiting as wary fish swim by, make an error, and get caught. (Page xi)

And the targets who succumb to the phishing are the *phools* in the book's title.

The examples of phishing for phools that Akerlof and Shiller discuss are all perfectly legal activities. If people were rational, there would be nothing about these activities to complain about. Such activities would then consist of the typical win-win voluntary exchanges between buyers and sellers that textbook economics endorses. And that's why it is hard to end phishing by banning this or that economic activity. There is no sense in shutting down, say, the entire financial sector and deprive rational people of opportunities for honest and gainful financial activity, simply to protect the phools who may be in danger of losing their life savings to some Ponzi schemer.

Pretty much any economic activity—say, the sale of clothes—can have a benign form (when the buyer is rational) and a phishing form (when the buyer is a shopaholic who can be manipulated by salespeople into buying massive amounts of expensive clothing that he/she would hardly ever wear).

Even the sale of cigarettes may be to the genuine benefit of the buyer if the buyer is not an addict and the benefit (pleasure) exceeds the cost (health risk). So, policy makers would have to take situation-specific approaches, such as a ban on cigarette advertising (the obvious vehicle for phishing in the case of smoking) or a ban on cigarette sales to minors (the obvious group identifiable as especially susceptible to phishing). Even nationalization—such a dirty word!—may make sense in a phishing-for-phools world. Nationalization of the cigarette industry may be a legitimate policy option because it would replace the profit-driven private sector with the profit-blasé public sector, with the latter presumably less interested in using phishing techniques to snare unwary consumers.

The basic problem is (a) that the seller of a good or service is usually interested only in his/her own profit and not in the welfare of the buyer, and (b) that the buyer may ignore his/her own best interest and act instead on what Akerlof and Shiller call his/her monkey-on-the-shoulder preferences. A profit-motivated seller may quite innocently have sold what a buyer had asked for. And the seller may have been totally unaware that the buyer was under the sway of his/her monkey-on-the-shoulder (hereafter, MOTS) preferences. In that case, phishing does occur, but in a passive way. Similarly, a seller may experiment repeatedly, not knowing what product or service would appeal to buyers, until something clicks with buyers' MOTS preferences.

The phishing gets more serious when the seller understands that the product or service he/she is selling could not possibly be good for the buyer, but sells it anyway in order to make a buck. This is a more active kind of phishing.

The phishing gets still more exploitative if the seller takes actions—such as manipulative advertising or product design that specifically appeals to buyers' MOTS preferences—to induce the vulnerable and suggestible buyer to buy things that are not in the buyer's best interest. (This is more in line with the definition of phishing in the quote from Akerlof and Shiller given above.)

None of this phishing is necessarily illegal or criminal, but the economic consequences for both efficiency and equity can be large.

The Economic Effects of Phishing

Let's take efficiency first. Economists at least since Adam Smith have argued that the free-market economic outcome is guided by the invisible hand of the marketplace to a *socially* efficient outcome even when every economic agent pursues his/her *self*-interest and is neither guided nor compelled by someone representing society's interest. This idea has received a formal statement called the First Welfare Theorem (FWT) in the work of several economists including Kenneth Arrow and Gerard Debreu.

Under the assumptions of the FWT, a free-market economy is a—pardon the jargon—a Pareto optimum. That is, a hypothetical social planner who has full control over all available productive resources and the best available technologies, and has a full understanding of what makes everybody truly happy, would nevertheless be unable to improve upon the free-market outcome, in the sense that our hypothetical social planner would be unable to make someone more happy—than the happiness he/she would attain in the free-market outcome—without making someone else less happy.

Now, in the phishing-for-phools economy of Akerlof and Shiller, people make decisions based on their monkey-on-the-shoulder preferences instead of their true preferences, where by "true preferences" I mean preferences that represent rational expectations of the consequences of consumption. In such an economy, the FWT would still be true, but only if the notion of happiness is based on people's MOTS preferences rather than their true preferences. The possibility would therefore exist for the hypothetical social planner to engineer an outcome in which some people are better off (than in the free-market outcome), and nobody is worse off, where the notions "better off" and "worse off" are based on the true preferences rather than the MOTS preferences.

To cut a long story short, the economy's scarce resources would be inefficiently used in the phishing-for-phools economy. This is no surprise considering that people's choices are based on their MOTS preferences. The misallocation may be especially damaging in the case of persistent addiction-driven expenditures and big-ticket expenditures—for example, wedding ceremonies, purchases of cars and homes, etc.—that occur only a few times in a person's life and therefore afford few opportunities for learning from one's mistakes.

Phishing for phools may also make society less fair. Sendhil Mullainathan and Eldar Shafir have argued that poor people tend to be vulnerable to a phenomenon called tunneling, whereby the poor, who often find themselves in desperate situations, spend their scarce resources on needs that are immediate, and tend to ignore needs that are important but not immediate.[3] Consequently, poor people may be particularly vulnerable to phishing scams. Phishing therefore may enable the rich to get richer at the expense of the easily-phishable poor.

Feasible Policy Responses

Given these consequences, what could policy makers do? Not a whole lot, as it turns out.

As we have already seen, banning certain economic activities outright or restricting them to the non-profit sector or the public sector may work in specific situations.

While economists tend to frown upon public-sector firms doing things that private-sector firms are able to do, Akerlof and Shiller's concept of phishing should make us look at public-sector firms—and even at the near-taboo policy of nationalization—in a brighter light. Being less profit-minded than private-sector firms, public-sector firms would surely be less likely to phish for the phools among their customers.

For example, one can make the argument that public-sector banks in India have protected people from being phished for phools by loan sharks who may offer seemingly reasonable loans to non-numerate people who have a poor understanding of compound interest, only to ruin them financially in the end. And it is not just loan sharks. It may very well be the case that the mere presence of public-sector banks as an available alternative has made India's private-sector banks refrain from practices that would have given them a reputation for phishy business.

But once again we must not get carried away in boosting the role of public-sector firms in the name of fighting phishing. Policy makers can squeeze the private sector to their hearts' content, but the profit motive will remain in the minds of people. Deprived of the chance to pursue profit through legitimate private-sector businesses, people may devote their energies to phishing schemes away from the government's gaze.

---

[3] *Scarcity: Why Having Too Little Means So Much* by Sendhil Mullainathan and Eldar Shafir, Times Books, New York, NY, 2013.

So, what else could policy makers do to fight phishing? The government could require businesses to provide money-back guarantees for any reason whatsoever (and not only for products that are clearly defective). But even here, careful situation-specific thinking will be necessary. While money-back guarantees would enable the phools to recover from a mistaken purchase, we need to impose some costs on the phools so they would make an effort to not make careless purchases in the first place. In other words, we must not open the door to what economists call moral hazard. After all, it is not costless for vendors to deal with people buying stuff and then returning them when they realize the purchase was a mistake. And those costs end up raising prices for everybody, phools and non-phools.

Another way to address phishing is to raise awareness about the tactics that phishers use to trap phools. This has no downside: sunshine, we all know, is the best disinfectant. Various government and non-profit institutions that provide information about products, services, business practices—e.g., the Better Business Bureau, Consumer Reports magazine, and a veritable alphabet soup of government regulators and watchdogs—are described by Akerlof and Shiller in Chapter Eleven ("The Resistance and Its Heroes") of their book. Nowadays, the Internet has made it possible for people to broadcast to the whole world their retrospective assessments—of both happiness and regret—of their shopping choices. This may no doubt help others avoid getting phished.

Moreover, public discussion on the Internet of a product, or service, or of firms' business practices, may vastly increase businesses' incentives to refrain from phishing.

However, even in this seemingly straightforward case, two notes of caution are needed: the public good nature of information and the phenomenon that Akerlof and Shiller call reputation mining.

Although copyright law can protect an author from pirates who produce knock-off copies for sale, the kind of consumer information we are discussing here will generally not have such legal protection. If a newspaper spends substantial resources to uncover commercial chicanery, the whole world—even the people who do not buy copies of the newspaper—would get to know about it. The newspaper that publishes the exposé would not be able to appropriate the full commercial value of its investigative work; other news sources that publish second-hand accounts of the original investigative report would benefit without having done the hard work. In this way, the non-excludable and non-rival nature of information would make free-riding the norm. The only systemic remedy would be regulatory and investigative work done directly by the government.

Retail web sites such as amazon, flipkart, alibaba, yelp, etc., publish freely provided customer reviews that can be candid, informative, and useful. But it is unclear whether the sites censor the reviews they do not like. And it is unclear whether these customer reviews are a good substitute for systematic investigations.

Moreover, as Akerlof and Shiller show by means of several examples, the endorsements for excellence that a commercial product or institution may receive in media reports, online comments, or word-of-mouth, may backfire because they carry within them a huge incentive to phish for phools. A shepherd patiently raises a goat from baby to adult, and then slaughters it for its meat. Likewise, a business that has patiently built up a reputation may eventually cash in on that reputation and phish its trusting clients for phools. The longer and more steadfast a firm's commitment to excellence, the higher would its reputation be among its clients and potential clients. And at some point the temptation may become overwhelming to cash in on the hard-earned reputation by selling a cheaply produced and substandard product to customers lulled by the company's sterling reputation. In other words, the same valuable information dissemination and consumer education that helps consumers distinguish between good and bad businesses may carry within it the incentive that turns good businesses bad.

A corollary is that government regulators and other watchdogs on the lookout for phishing should not go easy on a firm simply because it has a reputation for probity. Indeed, businesses with a reputation for good behavior may warrant even greater scrutiny.

So, ultimately, the only option may be for government agencies to engage in a perpetual game of whack-a-mole against egregious cases of phishing. Phishing stays within the law; so you can't send the phishermen to jail. You can only make new laws to stop the continued use of particular phishing strategies.

But once again, the obligatory reminder: a danger of anti-phishing regulatory scrutiny is excessive red tape. Policy makers must go after phishing without hindering legitimate business activity. Indeed, putting the squeeze on legitimate business activity may *increase* phishing by reducing the scope for people to make a good living in an honest way.

Who Will Support the Fight Against Phishing?

Now, strong anti-phishing policies cannot be sustained without political support for it. Although businesses are generally allergic to government regulation, they may support anti-phishing regulation if they can be persuaded that legitimate business activity would not be hurt, and that a government crackdown on phishing would lead to higher trust among customers and therefore to higher spending by them.

As for consumers, although they are likely to support anti-phishing regulation, one cannot take their support for granted. Not all consumers are equally vulnerable to phishing. Some are phools and some are not. And careful non-phools may stand to gain from the phoolishness of the phools. Consequently, they may take the side of the business sector if and when the government tries to crack down on phishing. To see why, let us consider Akerlof and Shiller's extended discussion of the US credit card industry in their fourth chapter ("Rip-offs Regarding Cars, Houses, and Credit Cards").

As we all know, paying with a credit card is more convenient than paying by cash or check. But credit card companies charge businesses substantial service fees whenever a customer pays by credit card. In the early days, businesses passed these service fees on to credit card-using shoppers by charging them an additional amount equal to the service fees. But later, credit card companies lobbied the US government to introduce a law—called the "Truth in Lending" law!—that required businesses to charge all shoppers the same whether they paid in cash or with a credit card. As a result, those who paid in cash in effect subsidized those who paid with credit cards.

As one would expect, credit card use skyrocketed, as shoppers no longer had to pay extra for the use of credit cards. A side effect of this expanded credit card use was increased spending. Study after study has shown that, with all other relevant factors controlled for, shoppers spend more when they use credit cards than when they use cash. Businesses loved the increased spending that came with the increased use of credit cards. Consequently, even after the Truth in Lending law was revoked—and businesses were once again allowed to charge shoppers more for the use of credit cards—businesses continued to charge all shoppers the same whether they paid by credit card or not.

And this is still the more or less universal practice in the US today.

To Akerlof and Shiller, this is an egregious case of phishing for phools. Businesses know that people spend more when they use credit cards. And businesses know that there is no rational basis for this phenomenon; it is a psychological weakness, a failure of rationality. And yet they charge shoppers the same price for cash purchases and credit card purchases—despite the steep service fees businesses must pay when shoppers pay by credit card—for no reason except to get more people to use credit cards, a practice that is for many a debt trap.

Some people spend in moderation when they pay in cash but lose all restraint when they shop with credit cards. Many of these people—Akerlof and Shiller's phools—consequently pile up huge debts to the credit card companies, and at astonishingly high interest rates. The interest payments collected from the phools not only swell the profits of the credit card companies, they also benefit the non-phools—i.e., the rich and/or careful shoppers who regularly pay off their credit card bills in full and never incur any debt to the credit card companies.

Why would the non-phools benefit from the phishing of the phools? Recall that businesses raise their prices to recoup the service fees charged by the credit card companies. Now, the credit card companies use their interest income (received, remember, from the phools who pile up large debts to them) to reduce their service fees. The more interest income the credit card companies earn from the indebted phools, the lower they can keep their service fees. And this reduces the prices of goods and services for *all* consumers, the phools as well as the non-phools. As a result, the non-phools benefit when phools get into debt and end up paying huge amounts in interest to the credit card companies.

So, returning to the issue of political support for anti-phishing regulation, one should expect opposition not only from the businesses that do the phishing but also from the non-phools who may benefit when the phools get phished.

It's tragic, but that's the way it is. Phools can expect solidarity and support neither from the businesses that phish them nor from their fellow shoppers who happen to be savvy. In a moral world, the non-phools who pay their credit card bills on time and in full—and therefore benefit from the lackadaisical behavior of the phools who pile up credit card debt—should protest the system's unfairness, even though they benefit from it. They should call upon businesses to end the current system of charging the same for cash purchases and credit card purchases. Or they should call upon credit card companies to stop charging businesses altogether and instead charge service fees only to shoppers who use credit cards. After all, given that the shoppers who use credit cards are the ones who enjoy the convenience of credit cards, they should bear the full costs of the credit card companies that provide the convenience.

But how likely is it that the non-phools would rise up and fight for the phools? Not very likely.

And speaking of moral behavior, the businesses that phish for phools are often major corporations, with their profits going to millions of shareholders. You would think that these shareholders would take responsibility and sack the managers who engage in phishing. But, again, how likely is that to happen? Indeed, it is not entirely unlikely that managers may be *promoted* precisely for their *lack* of scruples about phishing. It may actually be easier to rise up the ranks in a modern corporation by displaying a willingness or even an eagerness to phish for phools. After all, phishing is profitable, and what shareholder does not like dividends and capital gains?[4]

So, in the end, it is the government that will need to step in and compel retailers to charge shoppers who pay in cash only the price of the commodity and shoppers who pay by credit card an additional amount equal to the fees charged by credit card companies for credit card use. Neither the credit card industry nor the retail business sector would welcome this government intervention. The non-phools among shoppers would not be appreciative either, given that they benefit from the status quo.

And, in any case, an intervention-minded government would very likely also face an uphill struggle against the instinctive ideological opposition to all kinds of government regulation that dominates many of today's societies.

Akerlof and Shiller argue that the anti-government, anti-regulation bias that pervades our conventional wisdom is itself an instance of phishing for phools. They argue that this particular case of phishing is perpetrated by the media. The media are in the business of making money. They know that stories of dedicated, hard-working bureaucrats toiling away on behalf of the

---

[4]See the following reports of a study by Nathan Brooks, an Australian forensic psychologist: "1 in 5 CEOs are psychopaths, study finds" by Jonathan Pearlman, The Daily Telegraph, 13 September 2016. http://www.telegraph.co.uk/news/2016/09/13/1-in-5-ceos-are-psychopaths-australian-study-finds/, and "One in five CEOs are psychopaths, new study finds" by Harriet Agerholm, The Independent, 13 September 2016, http://www.independent.co.uk/news/world/australasia/psychopaths-ceos-study-statistics-one-in-five-psychopathic-traits-a7251251.html. See also https://www.psychology.org.au/news/media_releases/13September2016/Brooks/.

public, for salaries that are a lot lower than what they could earn in the private sector, do not sell well. Tales of scandal, corruption, incompetence: that's what sells. And so the media feeds the people—who, let's not forget, are governed by their MOTS preferences—a steady stream of tales of government incompetence and venality. Consequently, people tend to develop an allergy towards any kind of government intervention. They get phished into ignoring the benefits of the regulation that governments do on behalf of consumers.

To Akerlof and Shiller's critique of the media's manufacture of knee-jerk anti-regulationism, one may add a similar but older argument by John Kenneth Galbraith in *The Affluent Society*. Galbraith argued that the general public's preferences are manufactured by advertising. Moreover, almost all the advertising is done by the private sector, and all of it is a seamless paean to the great things the private sector does for us. Governments, bureaucracies, and regulators, on the other hand, never advertise. Consequently, the idea that the private sector may need to be reined in, and that it is the government's regulators who may need to do the reining in, never occurs to the general public.

Here's Galbraith discussing the "private affluence and public squalor" that he observed in 1950s America:

> He [the citizen] is subject to the forces of advertising and emulation by which production creates its own demand. Advertising operates exclusively, and emulation mainly, on behalf of privately produced goods and services. Since management of demand and emulative effects operate on behalf of private production, public services will have an inherent tendency to lag behind. ...
>
> ... Every corner of the public psyche is canvassed by some of the nation's most talented citizens to see if the desire for some merchantable product can be cultivated. No similar process operates on behalf of the non-merchantable services of the state.[5]

Akerlof and Shiller discuss other instances of the public discourse getting distorted when businesses buy a disproportionate share of the public's attention. Chapter Six ("Phood, Pharma and Phishing") describes how Merck, a pharmaceutical firm, orchestrated the launch of Vioxx, a new pain medication that it had developed. Merck's publicity strategies included the use of hired ghostwriters for journal articles in the names of influential doctors, and sponsored journal articles that were not labeled as such. The whole effort was aimed at phishing the physicians—sophisticated people, mind you; not the average person on the street—into prescribing Vioxx for their patients. All this was done despite very early indications that the drug was associated with heart attacks. Eventually, the drug had to be withdrawn: "The toll in the United States, as estimated by David Graham, was 88,000 to 139,000 heart attacks, with deaths conservatively estimated in excess of 26,000." (Page 90)

[5] *The Affluent Society*, by John Kenneth Galbraith, Fourth Edition, 1984, Houghton Mifflin Company, Boston, page 198. (First edition published in 1958.)

Drug ads in the United States are yet another example of phishing—perfectly legal, but cruelly manipulative of people's mental frailties. Television ads for a drug will typically extol the virtues of the drug through uplifting visuals of attractive actors testifying to some dramatic transformation in their lives thanks to the drug. For example, an allergy-ridden woman may be shown confined to a drab life indoors. Later that same woman, now suddenly beatific, may be shown traipsing over glorious meadows with her ecstatic children and her bouncy golden retriever in tow. Towards the end of the ad, the soothing voice of a voice-over actor would satisfy the government's regulatory requirements for disclosure by rapidly reading out a long list of side effects. But that soothing voice and the joyous visuals—which keep rolling while the list of side effects is being read—typically make it impossible for any awareness of the side effects to take root in the viewer's mind. The advertisers know this, and their ads are designed to numb the viewer to the side effects. Needless to say, the side effects would not have been mentioned at all but for the government's regulations.

In Chapter Eight ("Tobacco and Alcohol"), Akerlof and Shiller describe how the tobacco industry in the United States reacted to the emerging evidence of a link between smoking and lung cancer:

> "The industry could not refute the findings that lung cancer patients were much more likely to smoke than matched controls; nor that scientific evidence showed a relationship between cigarette tars and cancer. They followed the advice of Hill and Knowlton [a public relations firm] to do the next best thing. They created doubt."

No matter how strong the evidence against smoking, the tobacco companies would always find some scientist or physician who would play up some nit-picky unresolved issue. The financial clout of the tobacco companies ensured that these doubters got media coverage out of proportion to the scientific significance of their arguments.

And the media played along with this phishing. The media makes money by grabbing an audience. And that is best accomplished through the staging of fights. And a good fight requires two sides of roughly equal strength. So, the media gave equal coverage to those blaming smoking and to those saying that smoking was being unfairly blamed. The media were not doing this to serve the best interests of the audience. They were phishing for phools.

In a chapter titled "Conclusion," Akerlof and Shiller develop this depressing theme—of the power of what business wants the truth to be to drown out the power of what the truth really is—into a brave argument against the iconic notion of unrestricted free speech. In US law, the freedom to spend money to propagate one's views is considered as inviolable as the right to free speech itself. Swimming against the current, Akerlof and Shiller argue that this notion ignores the idea that speech can be used to phish as well as inform: "But just as phishing for phools yields a downside to free markets, similarly, it yields a downside to free speech." While agreeing that "speech is an essential mechanism of democracy," they add the following: "Speech is also a way to convince other people to act in *our* interests. If people are phishable, it is also a way to convince them to behave in a way that is in our interest, but not necessarily in *theirs*."

This argument leads them to a shockingly controversial policy proposal: "Metaphorically, we must place some limits on those with the resources to unleash huge loudspeakers that can drown out the message of less well-endowed others."

The fight against phishing will require public discussion and what is often referred to as awareness-raising. But that would require the assistance of the mass media. And it is by no means clear that the media will play a helpful role.

The Link between Behavioral Economics and Phishing

To Akerlof and Shiller, it is the moral obligation of a business to figure out what its customers truly need, and not what its customers could be persuaded to buy. Saying that customers know best what's good for them and then catering to their MOTS preferences is not good enough—it is phishing, plain and simple. Tempting people with advertisements that do not tell the whole unvarnished truth and instead appealing to people's MOTS preferences is not acceptable—it is phishing. Doing something to your customers that you would not want done to you is not acceptable—it is phishing. Telling people not the whole truth but only what you want them to hear or telling them what *they* want to hear, is not acceptable—it is phishing.

Selling people cigarettes is phishing, especially if all relevant information about smoking is not provided to customers in a maximally salient manner. Selling Cinnabons that are fragrant and tasty but frighteningly laden with calories is phishing, especially in situations where potential customers could not reasonably be expected to carefully weigh the costs and benefits. Selling a financial asset—or indeed pretty much anything: a used car, a new car, an insurance policy, a house, a diamond ring, whatever—without making sure that the customer fully understands the full implications of the purchase is phishing.

Akerlof and Shiller provide numerous other examples of what they consider phishing.

Here's one:

> "In one example [of marketers and advertisers exploiting the role of the subconscious in decision making, taken from *Hidden Persuaders* by Vance Packard], the makers of cake mixes appealed to housewives' desire for creativity by unnecessarily requiring the addition of an egg." (Page 7)

They retell a story told by Robert Cialdini, a psychologist, of a ploy once used by his brother Richard, who bought used cars, cleaned them up, and resold them:

> "Richard did not, as most of us would do, schedule his prospective buyers to come at different times. Instead, intentionally, he scheduled them to overlap. Each buyer … was then apprehensive that he might lose out: that other guy might get *his* car." (Page 7)

Akerlof and Shiller say that today's computerized slot machines are "addictive by design":

> "Ten years ago deaths due to cardiac arrest were an especially serious problem in the casinos. The emergency crews could not get through. Finally, the casinos created their own specially trained defibrillation teams. One surveillance video shows why such special

> training was necessary. In the video, as a squad from the casino defibrillates the heart arrest of a fellow player, the surrounding players play on, their trance unperturbed, even though the victim is literally at their feet." (Page ix)

Processed food companies are also following the "addictive by design" formula:

> "Big Phood commissions scientific laboratories to calculate consumers' "bliss points" that maximize their craving for sugar, salt, and fat. Yet no one wants to be obese.[6]" (Page xv)

Health clubs or gyms in the US usually offer a choice of two pricing plans: a flat fee per visit plan and an unlimited-visit plan for a larger lump-sum fee. Most people opt for the unlimited-visit plan, convinced that they would be assiduous exercisers. In reality, as the economists Stefano Della Vigna and Ulrike Malmendier recounted in a famous paper, most people go to the gym so infrequently that they would have saved money with the per-visit fee plan.[7] Akerlof and Shiller add:

> "Furthermore, the losses from this wrong choice were significant: $600 per year, out of average payments of $1,400. Additionally, to add insult to injury, the health clubs put roadblocks in the way of cancellation. Of the 83 clubs offering automatic monthly renewal in the Della Vigna-Malmendier sample, all accepted cancellation by personal appearance; but only 7 would accept cancellation by phone. Only 54 would accept a letter; and, of these, 25 required it to be notarized."

Clearly, health club managers were aware that their members were plagued by overconfidence. And yet they are preyed on this weakness. In other words, they went phishing.

In all these examples—and in the numerous other examples discussed throughout the book—people are being prodded by their profit motive to exploit the mental weaknesses, the predictable irrationalities, of others. This underlines the deep link between phishing for phools and the still-relatively-new field of behavioral economics, which studies those predictable irrationalities.

The cake mix example exploits the so-called *endowment effect* (or, a narrower version called the Ikea effect—people get attached to things they've had a hand in making). Robert Cialdini's brother was exploiting people's *loss aversion*. The health club story beautifully illustrates *hyperbolic discounting* (or patience for the long term and impatience for the short term). For every mental weakness cataloged and analyzed in a behavioral economics textbook, there is a phishing strategy that would tickle the profit motive of some entrepreneur.

Indeed, it seems to me that, going forward, it will be pretty much impossible for behavioral economics courses to avoid teaching *Phishing for Phools* and wrestling with its policy prescriptions. Instructors who feel comfortable with the pure rationality assumption would

---

[6] The authors occasionally take their practice of replacing "f" by "ph" to extremes.

[7] DellaVigna, Stefano, and Ulrike Malmendier. 2006. "Paying Not to Go to the Gym." American Economic Review, 96(3): 694-719. DOI: 10.1257/aer.96.3.694

probably see the book as a compendium of eccentric amusements. But, those who take the findings of behavioral economics seriously must now contend with the toxic cocktail created by the collision of the profit motive and the predictable mental weaknesses within us.

Conclusion

The book is beautifully, simply, and clearly written, with neatly laid out arguments and numerous illustrative examples. There's not a single equation in the entire book, which is surprising, considering that the authors are both academic economists and winners of the economics Nobel. The book needs to find a broad audience. But academic economists should pay special attention.

In *Phishing for Phools*, George Akerlof and Robert Shiller have made a strong argument that economists must contend seriously with the dark side of the profit motive. It's all very well to wax eloquent about the creative and regenerative aspects of the profit motive. But one cannot avoid the notion that the pursuit of profit may also lead people to exploit the mental weaknesses in people. Economists have studied crime and corruption. But phishing is different, more insidious and elusive. It is the dark art of staying within the law and laying traps for the unwary to fall into. The policy prescriptions that flow from economists' analyses of crime and corruption are largely irrelevant in the area of phishing.

Phishing leads to misallocation of resources and reduced economic efficiency. It might even contribute to unfairness and increased inequity. It pollutes the process of public dialog that democracy depends on. It is hard to fight phishing; there is no magic bullet that can kill it. But we must perpetually be awake to this beast that is a part of us.

UGC ENLISTED JOURNAL NO.41277

First published in 2008, Victorian Journal of Arts, a peer reviewed, UGC enlisted, bi-lingual, multidisciplinary journal, has been publishing original research articles and book reviews that traverse a wide range of disciplines in the field of Humanities. Published bi-annually in January and July, the Journal has already found its niche in the academic world, attracting scholarly articles both from India and abroad. In selecting articles the journal is not prejudicial to any particular political, social or religious ideology. Victorian Journal of Arts is an open forum that embraces both hard-core discipline specific articles and articles with an inter-disciplinary approach.

Price: Rs. 200/-