Kai A. Konrad

Attacking and Defending Multiple Valuable Secrets in a Big Data World

Max Planck Institute for Tax Law and Public Finance
Working Paper 2019 – 05

May 2019

Max Planck Institute for
Tax Law and Public Finance

Department of Business and Tax Law
Department of Public Economics

<http://www.tax.mpg.de>

Working papers of the Max Planck Institute for Tax Law and Public Finance Research Paper Series serve to disseminate the research results of work in progress prior to publication to encourage the exchange of ideas and academic debate. Inclusion of a paper in the Research Paper Series does not constitute publication and should not limit publication in any other venue. The preprints published by the Max Planck Institute for Tax Law and Public Finance represent the views of the respective author(s) and not of the Institute as a whole. Copyright remains with the author(s).

Max Planck Institute for Tax Law and Public Finance
Marshallplatz 1
D-80539 Munich
Tel: +49 89 24246 – 0
Fax: +49 89 24246 – 501
E-mail: ssrn@tax.mpg.de
<http://www.tax.mpg.de>

Attacking and Defending Multiple Valuable Secrets in a Big Data World

Kai A. Konrad*

June 27, 2019

Abstract

This paper studies the attack-and-defence game between a web user and a whole set of players over this user's 'valuable secrets.' The number and type of these valuable secrets are the user's private information. Attempts to tap information as well as privacy protection are costly. The multiplicity of secrets is of strategic value for the holders of these secrets. Users with few secrets keep their secrets private with some probability, even though they do not protect them. Users with many secrets protect their secrets at a cost that is smaller than the value of the secrets protected. The analysis also accounts for multiple redundant information channels with cost asymmetries, relating the analysis to attack-and-defence games with a weakest link.

JEL: D18, D72, D74, D82

Key Words: OR in societal problem analysis, big-data, privacy, web user, conflict, information rents, valuable secrets, attack-and-defence, multiple attackers, multiple defence items, multi-front contest.

*Address: Kai A. Konrad, Max Planck Institute for Tax Law and Public Finance, Marstallplatz 1, D-80539 Munich, Germany. Email: kai.konrad@tax.mpg.de. I thank Geoffrey Brennan, Rafaela Hennigs, Biljana Meiske, and Massimo Morelli. The usual caveat applies.

1 Introduction

This paper studies the conflict over rents from privacy and the protection of ‘valuable secrets’ by an internet user who is subject to adversarial attacks from multiple sides in the context of big data and learning algorithms. Police, homeland security, tax administration, political parties, presidential candidates, employers, but also criminals might try to extract information about single web users and learn secrets which the web user would like to keep private.¹ The new information-processing technologies enlarge the scope for information acquisition and the scope for the protection and management of privacy. Information on web users’ activities can be tracked, collected, and processed, at some cost. This may induce countermeasures: the targeted users might want to expend effort to block access to their private information. They might decide not to have an account on Facebook, Twitter, YouTube or WhatsApp, to deactivate devices such as Microsoft’s *Cortana* or the Amazon *Alexa* or other learning and information-acquiring electronic personal assistants/algorithms. They can delete cookies, use privacy-preserving browsers or other privacy-preserving

¹The police may use information for security and profiling purposes; see, e.g., Broeders, Schrijvers, van der Sloot et al. (2017). Autocrat governments might collect information about their citizens to score them and identify regime critics and revolutionaries, or to incentivize them in a way that the regime might find desirable; see, e.g., Chen and Cheung (2017). On the use of big data by tax administrations see, e.g., Tian, Lan, Chao et al. (2016) and Kontos and Maragoudakis (2016). Political parties can use information about voter types to microtarget campaign information; see, e.g., Schipper and Woo (2017) and Endres and Kelly (2018). Employers may extract information about their prospective or current employees from their social networking sites; see, e.g., Clark and Roberts (2010), Roth, Bobko, Van Iddekinge et al. (2016), Richey, Gonibeed and Ravishankar (2018).

devices,² including professional privacy protection services.³ Defensive measures have costs: inconvenience costs, the cost of investment in skills and technology, or straightforward fees paid for privacy-preserving services. A web user knows along which dimensions he has "valuable secrets" that he would like to keep. The user must decide whether he wants to protect access to this information and which possible information channels to block. The attackers must decide whether they should try to invade privacy and find out possible secrets and along which channels.

Contests about privacy rents are not a new phenomenon. But the enhanced technological options for the manipulation of information reinforce existing property rights conflicts over private information and the rents attached to it. The analysis accounts for many of the specific characteristics of the privacy conflict in the world wide web. It reveals that the information-blocking activities of web users with many valuable secrets benefit web users who do not protect their secrets. Moreover, the analysis suggests that policy interventions that change the regulatory framework and reduce the cost of blocking cause different benefits for the different player types. Such cost reductions benefit not only player types with many valuable secrets to protect. The user types with very few secrets also benefit: even though they do not expend blocking effort, they keep their information rents from valuable secrets with a larger probability in the equilibrium.

From a structural point of view, this paper is a contribution to the study

²Vishwanath, Xu and Ngoh (2018) discuss Facebook users' countermeasures and their opportunity costs. Drouin, Miller, Wehle et al. (2016) find that one of the motives for lying on the internet in online venues is concern for privacy. See also Goldberg (2007), Shen and Pearson (2011), and Heurix, Zimmermann, Neubauer et al. (2015) for reviews on privacy-enhancing technologies.

³A professional reputation management industry has already emerged. See, e.g., the survey of consumer reports on such services by Uzialko (2018).

of attack-and-defence-games.⁴ A seminal contribution by Bier, Nagaraj, and Abhichandani (2005) studies the problem of a single attacker who is confronted with a system with parallel or serial components. A considerable literature studies important variants of this general problem. Some of the relevant dimensions are whether defence effort and resources expended by the attacker occur simultaneously or sequentially, whether a system has redundant components or whether each component is critical, and the payoff consequences of the successful attack of one or several of the components. Hausken and Bier (2011) provide a short survey and study attack as a public good to which several attackers can contribute. Their paper and the present paper use game theory tools that have been developed in the field of contest theory that emerged from the study of property-rights conflict.⁵ Starting with a seminal contribution by Nitzan (1991a), a major line of research approached conflict problems in which one or both conflict parties consist of several players.⁶ Starting with Clark and Konrad (2007) and

⁴The current paper is also a contribution to the rapidly expanding field of the economics of privacy. Acquisti, Taylor, and Wagman (2016) provide an overview that emphasizes internet sales business. Some of this literature touches upon the privacy contest this might involve (see, e.g., Montes, Sand-Zantman, and Valletti 2018 and Belleflamme and Vergote 2016).

⁵Tullock (1967) looked at lobbying by interest groups. Other applications have been discussed in diverse contexts such as patent races, procurement, advertising, sports, political campaigns and advertising. The theory is also studied in more abstract terms, with seminal contributions by Tullock (1980), Hillman and Riley (1989), and Baye, Kovenock, and de Vries (1996). For surveys see Konrad (2009) and Garfinkel and Skaperdas (2012).

⁶Much of this literature is about free riding inside the groups of defenders or attackers. Nitzan (1991b), Davis and Reilly (1999) and Hausken and Bier (2011) address the role of sharing rules inside the group in such contexts, Choi, Chowdhury, and Kim (2016) study power asymmetries in a framework with conflict within and between the groups and Herbst, Konrad, and Morath (2015) study the endogeneity of group formation among heterogeneous players.

Arce, Kovenock, and Roberson (2012), a different line of conflict research addressed a fundamental asymmetry between attack and defence in conflicts with multiple fronts: an attacker may succeed if he wins on one front. The defender needs to protect all fronts. Such *best-shot-against-weak-link* situations are quite common and emerge in many contexts.⁷ Several major contributions apply contest theory in the area of attack and defence, including Hausken and Bier (2011), Levitin, Hausken, and Dai (2014), Levitin, Hausken, and Ben Haim (2014), and Hausken (2017).

The present paper considers one player who defends up to n valuable secrets against attackers that correspond to these secrets. These attack-and-defence games are strategically linked: the information about all secrets travels along the same information channel. The defender's choice on whether or not to block this common information channel simultaneously affects the success probability of attack for all attackers. The defender's willingness to block information access might therefore depend on the number of possible attackers and on the number of this player's valuable secrets. In this framework, attackers do not have aligned interests and attack success is not a public good as in Hausken and Bier (2011). Another major characteristic of our framework is the information structure. The defender knows the number and composition of his or her valuable secrets. The attackers only know an a priori distribution from which the type of defending player is drawn. Each attacker also has to choose whether to attack, and, in case of attack, whether to attack along one or several channels. The crucial choice for the defender is whether to block the channel(s) to his or her valuable secrets, and if there are many channels of attack, which of these channels to block.

⁷Important contributions are Chowdhury and Topolyan (2016), Chowdhury, Lee, and Topolyan (2016) and Deck and Sheremeta (2012). Work on this structure in the context of networks is by Dziubiński and Goyal (2013, 2017).

Related issues of incomplete information play a role in Bier, Oliveros, and Samuelson (2007). In their setup one player can choose the defence efforts expended on two objects. An attacker observes these defence efforts, chooses which object to attack, and has a private valuation of the two objects. Hausken (2014) considers a related game which allows for a richer setup describing the attacker’s technology and resource constraints. These two papers highlight the important aspect that the values of contested objects can be private information. The specific application in the context of the world-wide web drives different assumptions: whether or not a defender has a secret along which of the multiple dimensions is his or her private information. Therefore, the web user’s privacy protection has an all-or-nothing property: if the user chooses privacy protection, this blocks the common information channel that each of the attackers might use to acquire information.

2 The framework

There are $1 + n$ players, denoted by D (the ‘web user’) and $A_1, \dots, A_n$ (the ‘attackers’). Player D may have several valuable secrets. These secrets characterize D ’s type. More formally, the set of possible types $\mathbf{w}$ of player D is $\mathcal{W} = \{0, 1\}^n$. This makes D ’s type an n -dimensional vector with coordinates 0 and 1. If $w_j = 1$, then D has a valuable secret on dimension j : something that is valuable for D if kept private from A_j , and valuable for A_j to learn about. If $w_j = 0$, then D has no valuable secret along this dimension and cannot lose from an information attack by A_j . Nature chooses D ’s type-vector by a draw from the set $\mathcal{W}$. For simplicity we assume that each component w_j is drawn independently from the same distribution, where η is the probability that D ’s type is $w_j = 1$ and η is the same for all dimensions j . Player D knows $\mathbf{w}$; the player knows which valuable secrets

he or she has. There are n counterparty players A_j , one for each dimension j . Player A_j knows that D 's type $\mathbf{w}$ is nature's draw from $\mathcal{W}$ in the way just described.

The n possible secrets correspond to the n players $A_1, \dots, A_n$: one can think of a person facing n different counterparties, belonging to n different spheres of life. Each of these counterparties (police, immigration authorities, inland revenue, employer, etc.) has specific interests and would like to have information on the user's characteristics in this specific dimension. The number of these counterparties defines the number of possible valuable secrets. The person may have something valuable to hide from the respective counterparty in none, one, several or even all these different dimensions. Each counterparty must decide whether or not to find out and try to tap into the available information channel.⁸ Variants of the model could look at a heterogeneous set of counterparties, some of which might be interested in several dimensions⁹, or at multiple counterparties interested in the same dimension.¹⁰

Players A_j can make an attempt to learn player D 's type $\mathbf{w}$, and thereby also what is D 's specific valuable secret in the dimension j which A_j is

⁸The person might also have further characteristics for which there is no interested counterparty. Such secrets can be disregarded in the analysis, as there are no counterparties that potentially attack the person to learn about these secrets.

⁹This is likely to change the equilibrium on the side of the attackers. The analysis here simplifies along this dimension and focuses on the various dimensions of heterogeneity among the types of player D .

¹⁰If several attackers might be interested in the same potential secret, say, secret j , this might cause rivalry among the attackers interested in the same secret. Or, if they can all benefit from learning the same secret, it can create a potential collective goods problem among them. Public good problems have been studied independently (see, in particular, Hausken and Bier 2011). A variety of assumptions can be made in this context – for instance about how attackers' efforts aggregate, what attackers know about each other, and whether they coordinate.

interested in. Player D can choose to block information access. These choices are made simultaneously by all players. A pure strategy of A_j is denoted by $a_j \in \{0, 1\}$, where $a_j = 0$ means that A_j does not try to tap information and $a_j = 1$ means that A_j expends an effort to tap information ('searches'). This effort is normalized to a cost of 1 unit. We denote a mixed strategy by σ_j . It is fully characterized by the probabilities $\rho_{A_j}(a_j)$ by which A_j chooses $a_j \in \{0, 1\}$. Player D chooses whether to block information or not. The choice is denoted by $b \in \{0, 1\}$, where $b = 0$ means that D does not block information acquisition, and $b = 1$ means that D effectively blocks. If D blocks, none of the players A_j can learn D 's type $\mathbf{w}$ by expending search effort. Blocking has a cost equal to $c > 0$. A mixed strategy β is fully characterized by the probability p_D by which D chooses $b = 0$.

Player A_j learns $\mathbf{w}$, and in particular $w_j \in \{0, 1\}$ (and implicitly what is the valuable secret which D might have in this dimension) if and only if

$$a_j - b = 1 \tag{1}$$

that is, if A_j searches and D does not block. The payoff of A_j is

$$\pi_{A_j} = \begin{cases} v_A - a_j & \text{if } a_j - b = 1 \text{ and } w_j = 1 \\ -a_j & \text{otherwise.} \end{cases} \tag{2}$$

There is a fixed cost that is normalized to 1 that has to be paid if $a_j = 1$,¹¹ and a value v_{A_j} from learning the valuable secret along dimension j , if there is such a secret. For simplicity we assume symmetry: $v_{A_j} = v_A$ for all j . No benefit is earned by A_j either if the information is not obtained or if the information is obtained, but $w_j = 0$. Player A_j does not gain a different benefit from finding out that $w_j = 0$ than from not searching.

¹¹Players A_j might physically collect the data themselves. Or players A_j might choose whether to pay a data broker. Whether A_j could find valuable information or whether what the data broker provides is valuable for A_j depends on whether D has a valuable secret and whether D protected his or her privacy.

The payoff of D is

$$\pi_D = \sum_{j=1}^n \lambda_j v_D - cb, \quad (3)$$

where $\lambda_j = 1$ if $a_j - b < 1$ and $w_j = 1$ and $\lambda_j = 0$ otherwise. Player D 's 'valuable secret in j ', if there is one at j and remains unrevealed, has a value of v_D for D , and so for each valuable secret that D has. The benefit is normalized to zero if A_j finds out about the valuable secret if there is one for dimension j . Equation (3) describes how the technologies of attack and defence cause a strategic link between the n dimensions of the defender's possible secrets. Blocking information access has economies of scope for D and these are larger the larger is the number of valuable secrets that D has. It will be this dimension that drives D 's self-selection into whether to expend privacy protection effort.

It will be useful to define a counting function for vectors with components that are either zero or one,

$$z(\mathbf{w}) = \sum_{j=1}^n w_j. \quad (4)$$

For a vector $\mathbf{w}$ the function z counts the number of valuable secrets of D . While z does not completely characterize D 's type, it sorts and partitions the possible types of D along the player's number of valuable secrets and this partition will be important in the characterization of equilibrium.

3 Equilibrium

For a characterization of a Bayesian Nash equilibrium the following intermediate result about an outcome from the choice of specific strategies will be useful.

Lemma 1: *Let ζ be an integer from the set $\{0, 1, \dots, n\}$. Suppose that player D with type $\mathbf{w}$ chooses $b = 0$ if $z(\mathbf{w}) < \zeta$, $b = 1$ if $z(\mathbf{w}) > \zeta$ and $b = 0$*

or $b = 1$ with probabilities p_ζ and $1 - p_\zeta$ if $z(\mathbf{w}) = \zeta$. If player A_j chooses $a_j = 1$ then

$$q(\zeta, p_\zeta) \equiv \sum_{k=1}^{\zeta-1} \frac{k}{n} \binom{n}{k} \eta^k (1 - \eta)^{n-k} + \frac{\zeta}{n} \binom{n}{\zeta} \eta^\zeta (1 - \eta)^{n-\zeta} p_\zeta \quad (5)$$

is the probability by which player A_j learns that D with a randomly picked type $\mathbf{w}$ has $w_j = 1$ and what this secret is.

In the Appendix a generalized version of the lemma is shown. Figure 1 depicts the function $q(\zeta, p_\zeta)$. It describes the probability that an attack by a player A_j will successfully uncover a valuable secret along the dimension j which player A_j cares about. It describes this probability for a particular structure of blocking behavior by which the types of player D are partitioned such that all player types with more than ζ secrets block, all player types with less than ζ secrets do not block, and the types with precisely ζ secrets randomize between blocking or not blocking with blocking probability $(1 - p_\zeta)$.

Lemma 2: *The function $q(\zeta, p_\zeta)$ is continuous, monotonically increasing in p_ζ for any given $\zeta \in \{1, \dots, n\}$, and $q(\zeta, 1) = q(\zeta + 1, 0)$. Furthermore, $q(0, p_0) = 0$ and $q(n, 1) = \eta$.*

Proof. Monotonicity and continuity of $q(\zeta, p_\zeta)$ in p_ζ for $\zeta \geq 1$ follow directly from the definition of the function. The continuity at $q(\zeta, 1) = q(\zeta + 1, 0)$ and the properties $q(0, p_0) = 0$ and

$$q(n, 1) = \sum_{h=1}^n \frac{h}{n} \binom{n}{h} \eta^h (1 - \eta)^{n-h} = \eta \quad (6)$$

follow directly from inserting into the definition of the function. ■

Lemma 2 describes that $q(\zeta, p_\zeta)$ is a smooth function that has a unique combination of (ζ, p_ζ) for which $v_A q(\zeta, p_\zeta) = 1$, i.e., for which the expected

Figure 1: Function $q(\zeta, p_\zeta)$ consists of linear segments. Each segment describes the value of $q(\zeta, p_\zeta)$ for given ζ and for increasing values of $p_\zeta \in [0, 1]$. Except for $\zeta = 0$ these segments have strictly positive slope and the different segments jointly form a monotonic and continuous function.

benefit of attack equals the cost of attack for each of the players A_j . We are now prepared to characterize the Bayesian Nash equilibrium:

Proposition 1 *Let $v_D > c$ and $\eta v_A - 1 > 0$. A Bayesian Nash equilibrium exists and is characterized as follows. Let (z^*, p_z^*) be the solution of*

$$q(z^*, p_z^*) = \frac{1}{v_A}. \quad (7)$$

Player D chooses $b = 0$ if $z(\mathbf{w}) < z^$, $b = 1$ if $z(\mathbf{w}) > z^*$ and a mixed strategy β^* with $b = 0$ or $b = 1$ with probabilities p_z^* and $1 - p_z^*$ if $z(\mathbf{w}) = z^*$. Players A_j choose a mixed strategy σ_j^* with $a_j = 0$ with probability $\rho_{A_j}^*(0) = (1 - c/(z^* v_D))$ and $a_j = 1$ with probability $\rho_{A_j}^*(1) = c/(z^* v_D)$. Expected payoffs are $E\pi_{A_j} = 0$ and*

$$\begin{aligned} E\pi_D &= z(\mathbf{w})(1 - \frac{c}{z^* v_D})v_D \text{ if } z(\mathbf{w}) \leq z^* \\ E\pi_D &= z(\mathbf{w})v_D - c \text{ if } z(\mathbf{w}) > z^*. \end{aligned} \quad (8)$$

Proof. A combination (z^*, p_z^*) with $q(z^*, p_z^*)v_A - 1 = 0$ exists for $z^* \geq 1$. This follows from $\eta v_A - 1 > 0$ and the continuity and monotonicity properties of $q(z^*, p_z^*)$ that are described in Lemma 2.

Consider the optimality of player A_j 's candidate equilibrium behavior, given the probability $q(z^*, p_z^*)$. By (7) the choice of $a_j = 1$ yields the expected payoff $q(z^*, p_z^*)v_A - 1 = 0$. This equals A_j 's payoff from $a_j = 0$. For given $q(z^*, p_z^*)$ player A_j is indifferent between $a_j = 0$ and $a_j = 1$. Randomization between these strategies with $\rho_{A_j}^*(0) = (1 - \frac{c}{z^* v_D})$ is an optimal reply for A_j .

Consider the optimality of D 's candidate equilibrium behavior, given that each A_j randomizes between $a_j = 0$ and $a_j = 1$ with probabilities $\rho_{A_j}^*(0) = (1 - \frac{c}{z^* v_D})$ and $\rho_{A_j}^*(1) = \frac{c}{z^* v_D}$. If player D has $z(\mathbf{w}) = 0$, then $b = 0$ is optimal (there is nothing valuable that D could protect). Consider next player types D with $z(\mathbf{w}) \geq 1$. Player D compares the expected payoff

$z(\mathbf{w})v_D - c$ from $b = 1$ with the expected payoff $z(\mathbf{w})(1 - \frac{c}{z^*v_D})v_D$ from $b = 0$. From this comparison player D with $z(\mathbf{w}) > z^*$ strictly prefers $b = 1$, player D with $z(\mathbf{w}) < z^*$ strictly prefers $b = 0$ and D with $z(\mathbf{w}) = z^*$ is just indifferent between the two. Hence, $b = 0$ is an optimal reply for D with $z(\mathbf{w}) < z^*$, $b = 1$ is the optimal reply for D if $z(\mathbf{w}) > z^*$ and the mixed strategy β^* is an optimal reply for D if $z(\mathbf{w}) = z^*$. This strategy, in turn, generates $q(z^*, p_z^*)$ as in (7). ■

Before we interpret the equilibrium, we note (and show in the Appendix) the following

Proposition 2 *The equilibrium that is characterized in Proposition 1 is unique within the set of symmetric Bayesian Nash equilibria if*

$$\sum_{k=1}^z \frac{k}{n} \binom{n}{k} \eta^k (1 - \eta)^{n-k} v_A \neq 1 \quad (9)$$

for all possible $z = 1, 2, \dots, n$.

Figure 1 illustrates the equilibrium. The choice (z^*, p_z^*) makes attackers indifferent whether to search for information. This is mapped by the intersection of $q(\zeta, p_\zeta)$ with the flat line $1/v_A$. A larger value v_A attributed to valuable secrets shifts the horizontal line $1/v_A$ down, causing that, in the equilibrium, a larger share of web user types invest in privacy protection. This is intuitively plausible: if the expected rents that can be appropriated by A_j by successful search are higher, this tends to make each player A_j more eager to collect information. For unchanged type-specific blocking behavior $q(z^*, p_z^*)$ the players A_j are no longer indifferent, but prefer search ($a_j = 1$) to not search ($a_j = 0$). To restore indifference for players A_j requires that a larger share of the user types choose to protect their valuable secrets. Table 1 gives numerical values for z^* if the probability that a player has a valuable secret at a given dimension is $\eta = 1/2$ for a collection of $n \in \{1, 2, \dots, 10, 15, 20, 50, 100\}$ and $v_A \in \{5, 10, 20, 100\}$.

$v_A \backslash n$	1	2	3	4	5	6	7	8	9	10	15	20	50	100
5	1	2	2	2	3	3	4	4	5	5	8	10	25	49
10	1	1	1	2	2	3	3	3	4	4	6	9	23	46
20	1	1	1	1	2	2	2	3	3	4	6	8	21	44
100	1	1	1	1	1	1	2	2	2	3	4	6	18	40

Table 1: The value of z^* for various values of n and v_A , keeping η at $1/2$. Scientific Workplace was used for the calculations.

The table illustrates two natural comparative static properties of the equilibrium and underlines the intuition that was just described: a higher value attributed to uncovered secrets corresponds with a smaller set of user types who never block in the equilibrium. Furthermore, the set of types with a smaller number of secrets that never blocks tends to be larger if the number of secrets that user types might have is larger.

4 Welfare and economic policy

A benchmark is needed to assess the welfare properties of the equilibrium. If $v_D > v_A$ and if welfare is defined as the sum of benefits minus costs, the first-best allocation outcome is described by $b = 0$ and $a_j = 0$ for all $j = 1, \dots, n$, and by an allocation of the valuable secrets to the web user. The resulting expected welfare is $n\eta v_D$. In comparison, in equilibrium the sum of economic benefits net of search costs and blocking costs is lower. Five reasons reduce the welfare in the equilibrium compared to this benchmark value. First, all user types with $z(\mathbf{w}) > z^*$ block and this is costly. Second, a user type with $z(\mathbf{w}) = z^*$ blocks with probability $(1 - p_z^*)$ and this is costly. Third, each of the n attackers has the cost of information acquisition if the

attacker chooses $a_j = 1$. In the equilibrium this sums to expected costs of $n\rho_{A_j}^*(1)$. Fourth, not all secrets are allocated to the player who values them most. Secrets of a user type $z(\mathbf{w}) < z^*$ are revealed with probability $\rho_{A_j}^*(1) = c/(z^*v_D)$. If D is of type $z(\mathbf{w}) < z^*$, this sums up to an expected welfare loss of $z(\mathbf{w})\rho_{A_j}^*(1)(v_D - v_A)$. Finally, the same logic applies for the secrets of a user type with $z(\mathbf{w}) = z^*$ if this type does not block.

Consider the welfare benchmark if $v_D < v_A$. In this case, an omniscient planner allocates the information about all secrets to the various attackers A_j and prevents all search activities and blocking activities. The welfare in this benchmark is $n\eta v_A$. However, more realistically, a planner would have to respect the information distribution, and/or the technologically determined cost of information acquisition. This makes a comparison more difficult for $v_D < v_A$. A clear welfare loss occurs in this case if A_j searches and D blocks, as this leads to costs of searching and blocking, but to the same allocation outcome for the valuable secrets as if A_j does not search and D does not block.

Policy interventions that marginally change the regulatory framework and reduce the cost of blocking affect the different user types in different ways. Such interventions leave the equilibrium values (z^*, p_z^*) unaffected, as $q(z^*, p_z^*)$ is constructed to make the attackers indifferent to whether to attack. User types with many valuable secrets ($z(\mathbf{w}) > z^*$) directly benefit from a reduction in c : they choose to block with probability 1 prior to and after such a cost change, and the policy intervention reduces their costs and leaves their benefits unaffected. A cost reduction is also good for user types with $z(\mathbf{w}) < z^*$. These types do not block, but a reduction in the cost c reduces the equilibrium probability $\rho_{A_j}^*(1) = c/(z^*v_D)$ of attack. For the case $v_D > v_A$ such a policy intervention is unambiguously welfare increasing. It does not change the sets of user types that block or do not block. It reduces

the blocking cost for user types who block and it makes attack less likely. The latter reduces the expected attack costs and makes it more likely that the valuable secrets of web users who do not take protective measures will remain undisclosed.

5 Redundant information sources

Suppose that players A_j can attempt to learn player D 's type $\mathbf{w}$ (and the secrets involved) from a number of m different information sources, indexed as $t \in \{1, \dots, m\}$.¹² Suppose each one of these sources can fully reveal $\mathbf{w}$. A pure strategy of A_j is a vector $\mathbf{a}_j = (a_{j1}, \dots, a_{jm})$ where $a_{jt} \in \{0, 1\}$. Now $a_{jt} = 0$ means that A_j does not try to tap source t for information and $a_{jt} = 1$ means that A_j expends a unit effort to tap source t for information. The set of all possible strategies $\mathbf{a}_j$ is T . The set T can be partitioned into the subsets $T^0, T^1, \dots, T^m$, where T^k is defined as the subset of T that contains all search strategies which have a sum of their components a_{jt} equal to k . For brevity, define also $\mathbf{0}^m = (0, 0, \dots, 0)$ and $\mathbf{1}^m = (1, 1, \dots, 1)$. A mixed strategy σ_j of attacker A_j is described by a probability vector that associates a probability $\rho_{A_j}(\mathbf{a}_j)$ to each strategy $\mathbf{a}_j \in T$, with $\sum_{\mathbf{a}_j \in T} \rho_{A_j}(\mathbf{a}_j) = 1$.

Player D chooses whether to block none, some, or all of the m possible sources of information.¹³ The vector $\mathbf{b} = (b_1, \dots, b_m)$ describes D 's blocking choices, where $b_t = 0$ means that D does not block information acquisition from source t , and $b_t = 1$ means that D effectively blocks this potential

¹²For instance, a Facebook account, matched with big data and properly exploited by learning algorithms might reveal D 's full profile just as well as the information obtained from *Cortana*'s recordings.

¹³Intuitively, think of D 's choice of closing his or her Facebook account, shutting off *Cortana* etc. A blocking action at source t , if taken, is assumed to be fully effective for this source such that none of the players A_j can learn D 's type $\mathbf{w}$ by expending effort on this specific source.

source of information. The costs to block the access to the information at the source t are $c_t > 0$ for the respective $t \in \{1, \dots, m\}$. Heterogeneity of blocking costs is plausible if we think of the nature and use-intensity of different web activities. The set of all feasible blocking strategies of D consists of the set of m -dimensional vectors with components that can take one of the two possible values 0 or 1. This set is also T . Player D can choose a mixed strategy. A mixed strategy β is described by a vector of probabilities such that the component $p_D(\mathbf{b})$ is the probability by which D chooses strategy $\mathbf{b}$, for all $\mathbf{b} \in T$, with $\sum_{\mathbf{b} \in T} p_D(\mathbf{b}) = 1$.

Player A_j finds out about a possible valuable secret that D might have along dimension j (along with the whole vector $\mathbf{w}$), if and only if

$$\max_{t \in \{1, \dots, m\}} (a_{jt} - b_t) = 1. \quad (10)$$

Player A_j finds out about D 's type $\mathbf{w}$ if A_j expends effort on extracting information from at least one source that is unblocked. Player A_j does not find out if, instead, $\max_{t \in \{1, \dots, m\}} (a_{jt} - b_t) < 1$. The condition (10) replaces (1) and describes a *weakest-link-against-best-shot* nature of the privacy contest.

Payoffs can now be written, similarly to (2) and (3) as

$$\pi_{A_j} = \begin{cases} v_A - \sum_{t=1}^m a_{jt} & \text{if } \begin{cases} w_j = 1 \text{ and} \\ \max_{t \in \{1, \dots, m\}} (a_{jt} - b_t) = 1 \end{cases} \\ -\sum_{t=1}^m a_{jt} & \text{otherwise} \end{cases} \quad (11)$$

for A_j and

$$\pi_D = \sum_{j=1}^n \lambda_j v_D - \sum_{t=1}^m c_t b_t \quad (12)$$

for D , where $\lambda_j = 1$ if $\max_{t \in \{1, \dots, m\}} (a_{jt} - b_t) < 1$ and $w_j = 1$, and $\lambda_j = 0$ otherwise.

For a characterization of equilibrium consider specific strategies of D and A_j that later turn out to be part of the equilibrium strategies. Let player D choose $\mathbf{b} = \mathbf{0}^m$ if $z(\mathbf{w}) < \zeta$, $\mathbf{b} = \mathbf{1}^m$ if $z(\mathbf{w}) > \zeta$, and mix between $\mathbf{b} = \mathbf{0}^m$

and $\mathbf{b} = \mathbf{1}^m$ if $z(\mathbf{w}) = \zeta$ with probabilities p_ζ and $(1 - p_\zeta)$. Furthermore, let players A_j choose strategies $\mathbf{a}_j \in T^1$ (i.e., they each attack at precisely one source). Then,

$$q(\zeta, p_\zeta) \equiv \sum_{k=1}^{\zeta-1} \frac{k}{n} \binom{n}{k} \eta^k (1 - \eta)^{n-k} + \frac{\zeta}{n} \binom{n}{\zeta} \eta^\zeta (1 - \eta)^{n-\zeta} p_\zeta \quad (13)$$

describes the probability that a randomly chosen player A_j who tries to tap one randomly chosen source learns that D with a randomly picked type $\mathbf{w}$ has $w_j = 1$ (and learns this valuable secret). This is shown formally in the Appendix. Moreover, in analogy to Lemma 2, $q(\zeta, p_\zeta)$ is continuous and monotonically increasing in p_ζ for any given positive integer $\zeta \geq 1$, and $q(\zeta, 1) = q(\zeta + 1, 0)$, and $q(0, p_0) = 0$ and $q(n, 1) = \eta$. This leads to a generalized version of Proposition 1:

Proposition 3 *Let $v_D > \sum_{t=1}^{t=m} c_t$ and $\eta v_A - 1 > 0$. The following Bayesian Nash equilibrium exists: The equilibrium strategy of D is characterized by a combination (z^*, p_z^*) that solves*

$$q(z^*, p_z^*) = \frac{1}{v_A}, \quad (14)$$

such that D places probability 1 on $\mathbf{0}^m$ if $z(\mathbf{w}) < z^$, probability 1 on $\mathbf{1}^m$ if $z(\mathbf{w}) > z^*$ and randomizes with probability p_z^* and $(1 - p_z^*)$ between $\mathbf{0}^m$ and $\mathbf{1}^m$ if $z(\mathbf{w}) = z^*$. Players A_j choose $\mathbf{0}^m$ with probability*

$$\rho_{A_j}^*(\mathbf{0}^m) = \left(1 - \frac{\sum_{t=1}^{t=m} c_t}{z^* v_D}\right) \quad (15)$$

and each $\mathbf{a}_j \in T^1$ with coordinate $a_{jt} = 1$ with probability $\rho_{A_j}^(\mathbf{a}_j) = c_t / (z^* v_D)$ for $t = 1, \dots, m$. Expected payoffs are $E\pi_{A_j} = 0$ and*

$$\begin{aligned} E\pi_D &= z(\mathbf{w}) \left(1 - \frac{\sum_{t=1}^{t=m} c_t}{z^* v_D}\right) v_D \text{ if } z(\mathbf{w}) \leq z^* \\ E\pi_D &= z(\mathbf{w}) v_D - \sum_{t=1}^{t=m} c_t \text{ if } z(\mathbf{w}) > z^*. \end{aligned} \quad (16)$$

Proof. Consider the optimal reply of player A_j for an arbitrary j , given D 's candidate equilibrium strategy. As D either blocks all sources or none of them, any strategy $\mathbf{a}_j \in T^k$ with $k > 1$ is strictly dominated by $\mathbf{a}_j \in T^1$. The payoff for A_j is zero for $\mathbf{a}_j \in T^0$. By construction of $q(z^*, p_z^*)$ each of $\mathbf{a}_j \in T^1$ yields expected payoff equal to

$$q(z^*, p_z^*)v_A - 1 = 0. \quad (17)$$

Hence, all $\mathbf{a}_j \in T^0 \cup T^1$ as well as their mixtures are optimal replies. This set of optimal replies includes the mixed strategy with

$$\rho_{A_j}(\mathbf{0}^m) = 1 - \frac{\sum_{t=1}^{t=m} c_t}{z^*v_D} \quad (18)$$

and with $\rho_{A_j}(\mathbf{a}_j) = \frac{c_t}{z^*v_D}$ for $\mathbf{a}_j \in T^1$ with $a_{jt} = 1$ and $a_{jk} = 0$ for all $k \neq t$.

Consider next the optimal reply of D to the attackers' candidate equilibrium strategies. The payoff for D with type $\mathbf{w}$ with a number $z(\mathbf{w})$ of secrets is a function of $\mathbf{b} = (b_1, \dots, b_m)$:

$$\begin{aligned} \pi_D(\mathbf{b}) &= \sum_{j=1}^{j=n} w_j v_D \left(1 - \frac{\sum_{t=1}^{t=m} c_t}{z^*v_D}\right) + \sum_{t=1}^{t=m} b_t \left(\sum_{j=1}^{j=n} w_j v_D \frac{c_t}{z^*v_D} - c_t\right) \\ &= z(\mathbf{w})v_D \left(1 - \frac{\sum_{t=1}^{t=m} c_t}{z^*v_D}\right) + \sum_{t=1}^{t=m} \left(b_t z(\mathbf{w})v_D \frac{c_t}{z^*v_D} - b_t c_t\right). \end{aligned} \quad (19)$$

The first term is D 's payoff if D does not block. All $z(\mathbf{w})$ secrets of D remain private with the probability (18). The second term adds the sum of the additional benefits and costs if $b_t = 0$ is replaced by $b_t = 1$ for the various t . If $b_t = 1$, then D blocks information source t at a cost c_t and pays this cost. This blocking activity helps against all searches at this t . Each of the n attackers searches at t with probability $c_t/(z^*v_D)$. Compared to not blocking at t , blocking yields D an additional value of v_D with probability $c_t/(z^*v_D)$ for each dimension for which $w_j = 1$. The second term sums up all these net benefits for the different t and for the different secrets that D

might have. The second line in (19) makes use of (4). Note that (19) takes into account that each attacker randomizes among $m + 1$ pure strategies: an attacker either does not attack anywhere or attacks at exactly at one randomly chosen source t . Note also that (19) is independent of whether different attackers correlate their attack behavior with each other or not. The second term in (19) can also be written as

$$\left(\frac{z(\mathbf{w})v_D}{z^*v_D} - 1 \right) \sum_{t=1}^{t=m} b_t c_t. \quad (20)$$

Compared to $b_t = 0$, the choice $b_t = 1$ increases D 's payoff if $z(\mathbf{w}) > z^*$. It decreases D 's payoff if $z(\mathbf{w}) < z^*$ and does not change D 's payoff if $z(\mathbf{w}) = z^*$. This holds for each t . Hence, D 's optimal choice is $\mathbf{b} = (1, \dots, 1)$ for $z(\mathbf{w}) > z^*$, is $\mathbf{b} = (0, \dots, 0)$ for $z(\mathbf{w}) < z^*$, and all $\mathbf{b} \in T$ or their mixtures lead to the same expected payoff for D if $z(\mathbf{w}) = z^*$. This makes the candidate equilibrium mixture an optimal reply for $z(\mathbf{w}) = z^*$. ■

The comparison between Proposition 1 and Proposition 3 shows that neither a larger number of different channels nor an asymmetry in the cost of protecting one or the other of these channels affects the qualitative nature of the equilibrium compared to the single-channel case: the web user either blocks all channels or none of them. As a consequence each attacker chooses at most one channel and is indifferent about which one to attack. In the equilibrium the attackers choose the various attack probabilities for the different channels at sizes that just compensate for the differences in D 's cost of blocking this channel. The multiplicity of secrets that a web user can protect by blocking leads to economies of scope for D for user types with a larger number of secrets. The multiplicity and redundancy of possible sources of information analytically works in the opposite direction, making blocking more costly.¹⁴

¹⁴The regimes with different numbers m of possible information channels might not be

6 Conclusions

This paper studies the privacy conflict between a web user on one hand and a whole set of attackers on the other. The contest is about potential information rents that are tied to web users' valuable secrets. We account for a multiplicity of different valuable secrets, where each attacker tries to unveil one specific secret. The web user might have few or many valuable secrets and this is the user's private information.

The multiplicity of secrets, and the heterogeneity of user types are of strategic value for the holders of these secrets. A user with many secrets will block information access, and the privacy rents of this user type will exceed the blocking costs. User types with an intermediate number of secrets are just indifferent between blocking or not blocking. Users with few secrets do not block.

An attacker who is considering whether to attack and find out the secret that a given user might have, does not know whether this is a user with many secrets (who protects his or her secrets) or a user with few secrets (who does not protect his or her secrets). If there were only web users with few secrets, and if all of them did not take any precautions, then the attackers would spend the costs and find out the secrets. But the attackers anticipate that the user blocks if the user has many secrets. In a way, the user types with few secrets can free ride on these user types with many secrets and benefit from their blocking behavior: in the equilibrium the attackers attack only with some probability. Hence, even web user types who do not protect their secrets will be attacked only with some probability. With the remaining probability they can enjoy the benefits of their valuable but unprotected

directly comparable, however. For instance, if blocking means not to use a particular web service, the cost of not using this service might depend on whether there is a substitute for it.

secrets.

Furthermore, multiplicity of redundant sources of information has been shown to cause a strategic disadvantage for the web user. This is mainly because the web user needs to protect all potential information sources ('weakest-link' property), whereas each of the attackers needs to tap into only one of these multiple sources to discover what he or she wants to discover ('best-shot' property).

7 Appendix

Proof of Proposition 2 To show uniqueness let us consider the optimal reply of A_j to the optimal reply of D to a given mixed strategy that is characterized by a symmetric choice of probability $\hat{\rho} \in [0, 1]$ for not attacking. This problem defines a self-mapping from $[0, 1]$ to $[0, 1]$. It is to be shown that this self-mapping has at most one fixed point, and that this fixed point also determines the probability that D blocks as a function of D 's type.

Player D 's optimal reply if the A_j 's have a probability $\hat{\rho}$ of not to attack depends on D 's type $\mathbf{w}$. Let $\hat{z}$ the real number that solves $\hat{z}\hat{\rho}v_D = \hat{z}v_D - c$ and define

$$z^-(\hat{\rho}) \equiv \min\{n, \text{integer}(\hat{z})\}. \quad (21)$$

Then player D blocks if $z(\mathbf{w}) > z^-(\hat{\rho})$ and does not block if $z(\mathbf{w}) < z^-(\hat{\rho})$. The player D with $z(\mathbf{w}) = z^-(\hat{\rho})$ also does not block if $z^-(\hat{\rho}) < \hat{z}$. If $z^-(\hat{\rho}) = \text{integer}(\hat{z}) = \hat{z}$, then the optimal reply is set-valued: this type of web user does not block with a probability $p_{z^-(\hat{\rho})} \in [0, 1]$ and blocks everywhere otherwise.

Turn now to the implications of this blocking behavior for the optimal choice of $a_j \in \{0, 1\}$. The expected payoff for A_j from $a_j = 0$ is zero. The

expected payoff for A_j from $a_j = 1$ is

$$E\pi_{A_j} = \left[\sum_{k=1}^{z^-(\hat{\rho})} \frac{k}{n} \binom{n}{k} \eta^k (1-\eta)^{n-k} \right] v_A - 1 \quad (22)$$

$$- v_A (1 - p_{z^-(\hat{\rho})}) \left[\frac{z^-(\hat{\rho})}{n} \binom{n}{z^-(\hat{\rho})} \eta^{z^-(\hat{\rho})} (1-\eta)^{n-z^-(\hat{\rho})} \right].$$

For values of $\hat{\rho}$ with $z^-(\hat{\rho}) = \text{integer}(\hat{z}) < \hat{z}$ all types D with $z(\mathbf{w}) \leq z^-(\hat{\rho})$ do not block and all types with $z(\mathbf{w}) > z^-(\hat{\rho})$ block. The summation term in the first line of (22) gives the resulting probability that $a_j = 1$ uncovers a valuable secret on dimension j to A_j , times the respective benefit v_A from this secret. The term -1 represents A_j 's unit cost of search. In Figure 2 the resulting payoff for A_j for these values of $\hat{\rho}$ is expressed by the step function consisting of the horizontal bars. For values of $\hat{\rho}$ with $z^-(\hat{\rho}) = \text{integer}(\hat{z}) = \hat{z}$ for player D with type $z(\mathbf{w}) = z^-(\hat{\rho})$ the player's reply is set-valued and any choice $p_{z^-(\hat{\rho})} \in [0, 1]$ is optimal for this type of player D . The possible values of $p_{z^-(\hat{\rho})}$ connect the horizontal bars in Figure 2 and make the locus of A_j 's payoff $E\pi_{A_j}$ from choice $a_j = 1$ a mapping of $(1 - \hat{\rho})$ into a set that is connected and downward sloping. It starts with a value $\eta v_A - 1$ for $(1 - \hat{\rho}) = 0$ and reaches -1 for $(1 - \hat{\rho}) = 1$.

Due to condition (9) the payoff $E\pi_{A_j}$ in any of the flat parts of $E\pi_{A_j}$ in Figure 2 is either positive or negative, but never zero.¹⁵ Player A_j compares

¹⁵Note that use of (9) is made here to exclude that the zero-line in Figure 2 passes through one of the flat segments. There is only a finite number of values of $\eta \in [0, 1]$ for which (9) does not hold. For any given z and n , the left-hand side of (9) is strictly increasing in η for all $\eta \in (0, \frac{1}{2})$ and strictly decreasing in η for all $\eta \in (\frac{1}{2}, 1)$ and it is symmetric around $\eta = 1/2$. Therefore

$$\sum_{k=1}^z \frac{k}{n} \binom{n}{k} \eta^k (1-\eta)^{n-k} = \frac{1}{v_A}$$

has at most two solutions for values $\eta \in [0, 1]$.

Figure 2: The expected payoff of a player A_j from attacking if player D expects a symmetric attack probability of $(1 - \hat{\rho})$ and optimally reacts according to D 's own type and to this anticipated attack probability.

the payoff from $a_j = 0$ (which is constant and zero for all $\hat{\rho}$) with the payoff from $a_j = 1$. Figure 2 illustrates that A_j prefers to choose $a_j = 1$ for all $(1 - \hat{\rho}) < (1 - \tilde{\rho})$. The player prefers to attack with probability 1, and this probability is higher than any $(1 - \hat{\rho}) \in [0, (1 - \tilde{\rho}))$. Furthermore, A_j prefers $a_j = 0$ for all $(1 - \hat{\rho}) > (1 - \tilde{\rho})$. Hence, A_j chooses to attack with probability 0 that is smaller than $(1 - \hat{\rho}) \in ((1 - \tilde{\rho}), 1]$. The only possible fixed point is at $(1 - \hat{\rho}) = (1 - \tilde{\rho})$. To be a fixed point, this requires a specific blocking probability for the indifferent web user type: the probability that makes A_j just indifferent between attacking and not attacking and this identifies the equilibrium that is described in Proposition 1. ■

Constructive proof of equation (13) For a construction of (13) consider the following inductive argument: For $\zeta = 0$ it holds that $q(0, p_0) = 0$ for all $p_0 \in [0, 1]$. Conditional on $z(\mathbf{w}) = 0$, the probability that A_j 's information acquisition $\mathbf{a}_j \in T^1$ at one source t successfully finds out that $w_j = 1$ is zero. This is independent of the strategy choice of D .

For $\zeta = 1$, by definition, all players with $z(\mathbf{w}) = 0$ choose $\mathbf{b} = \mathbf{0}^m$ and all players with $z(\mathbf{w}) \geq 2$ choose $\mathbf{b} = \mathbf{1}^m$. All players with $z(\mathbf{w}) = 1$ choose $\mathbf{b} = \mathbf{0}^m$ with probability p_1 and $\mathbf{b} = \mathbf{1}^m$ with probability $(1 - p_1)$. Hence, if A_j chooses an $\mathbf{a}_j \in T^1$, A_j will uncover that D has $w_j = 1$ (and what the secret is) with probability

$$q(1, p_1) \equiv q(0, 1) + \frac{1}{n} \binom{n}{1} \eta^1 (1 - \eta)^{n-1} p_1. \quad (23)$$

Here $q(0, 1) = 0$ has already been derived. In the second term on the right-hand side, $\binom{n}{1} \eta^1 (1 - \eta)^{n-1}$ is the probability that $z(\mathbf{w}) = 1$, and $\frac{1}{n}$ is the probability that the single component of $\mathbf{w}$ that is equal to 1 for this $\mathbf{w}$ is precisely the j -th component of $\mathbf{w}$, and p_1 is the probability that D with $z(\mathbf{w}) = 1$ chooses $\mathbf{b} = \mathbf{0}^m$.

For $\zeta = 2$,

$$q(2, p_2) = q(1, 1) + \frac{2}{n} \binom{n}{2} \eta^2 (1 - \eta)^{n-2} p_2. \quad (24)$$

Here, $\binom{n}{2} \eta^2 (1 - \eta)^{n-2}$ is the probability that precisely two components of the n components of $\mathbf{w}$ are equal to 1, and $2/n$ is the conditional probability that one of these two components is component j .

This logic generalizes for $\zeta = k$ to

$$\begin{aligned} q(k, p_k) &= q(k-1, 1) + \frac{k}{n} \binom{n}{k} \eta^k (1 - \eta)^{n-k} p_k \\ &= \sum_{h=1}^{k-1} \frac{h}{n} \binom{n}{h} \eta^h (1 - \eta)^{n-h} + \frac{k}{n} \binom{n}{k} \eta^k (1 - \eta)^{n-k} p_k. \end{aligned} \quad (25)$$

■

References

- [1] Acquisti, Alessandro, Curtis Taylor, and Liad Wagman, 2016, The economics of privacy, *Journal of Economic Literature*, 54(2), 442-492.
- [2] Arce, Daniel G., Dan Kovenock, and Brian Roberson, 2012, Weakest-link attacker-defender games with multiple attack technologies, *Naval Research Logistics*, 59(6), 457-469.
- [3] Baye, Michael R., Dan Kovenock, and Casper G. de Vries, 1996, The all-pay auction with complete information, *Economic Theory*, 8(2), 291-305.
- [4] Belleflamme, Paul, and Wouter Vergote, 2016, Monopoly price discrimination and privacy: The hidden cost of hiding, *Economics Letters*, 149, 141-144.
- [5] Bier, Vicki M., Aniruddha Nagaraja, and Vinod Abhichandani, 2005, Protection of simple series and parallel systems with components

of different values, *Reliability Engineering & System Safety*, 87(3), 315-323.

- [6] Bier, Vicki M., Santiago Oliveros, and Larry Samuelson, 2007, Choosing what to protect: Strategic defensive allocation against an unknown attacker, *Journal of Public Economic Theory*, 9(4), 563-587.
- [7] Broeders, Dennis, Erik Schrijvers, Bart van der Sloot, Rosamunde van Brakel, Josta de Hoog, and Ernst Hirsch Ballin, 2017, Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data, *Computer Law & Security Review*, 33(3), 309-323.
- [8] Chen, Yongxi and Anne S. Y. Cheung, 2017, The transparent self under Big Data profiling: Privacy and Chinese legislation on the social credit system, *Journal of Comparative Law*, 12(2), 356-378.
- [9] Choi, Jay Pil, Subhasish M. Chowdhury, and Jaesoo Kim, 2016, Group contests with internal conflict and power asymmetry, *Scandinavian Journal of Economics*, 118(4), 816-840.
- [10] Chowdhury, Subhasish M., and Iryna Topolyan, 2016, The attack-and-defense group contests: Best-shot versus weakest link, *Economic Inquiry*, 54(1), 548-557.
- [11] Chowdhury, Subhasish M., Dongryul Lee, and Iryna Topolyan, 2016, The max-min group contest: Weakest-link (group) all-pay auction, *Southern Economic Journal*, 83(1), 105-125.
- [12] Clark, Derek J., and Kai A. Konrad, 2007, Asymmetric conflict: Weakest link against best shot, *Journal of Conflict Resolution*, 51(3), 457-469.
- [13] Clark, Leigh A., and Sherry J. Roberts, 2010, Employer's use of social networking sites: A socially irresponsible practice, *Journal of*

Business Ethics, 95(4), 507-525.

- [14] Davis, Douglas D., and Robert J. Reilly, 1999, Rent-seeking with non-identical sharing rules: An equilibrium rescued, *Public Choice*, 100(1-2), 31-38.
- [15] Deck, Cary, and Roman M. Sheremeta, 2012, Fight or flight? Defending against sequential attacks in the game of siege, *Journal of Conflict Resolution*, 56(6), 1069-1088.
- [16] Drouin, Michelle, Daniel Miller, Shaun M.J. Wehle, and Elisa Hernandez, 2016, Why do people lie online? "Because everyone lies on the internet", *Computers in Human Behavior*, 64, 134-142.
- [17] Dziubiński, Marcin, and Sanjeev Goyal, 2013, Network design and defence, *Games and Economic Behavior*, 79, 30-43.
- [18] Dziubiński, Marcin, and Sanjeev Goyal, 2017, How do you defend a network?, *Theoretical Economics*, 12(1), 331-376.
- [19] Endres, Kyle, and Kristin J. Kelly, 2018, Does microtargeting matter? Campaign contact strategies and young voters, *Journal of Elections, Public Opinion and Parties*, 28(1), 1-18.
- [20] Garfinkel, Michelle R., and Stergios Skaperdas (eds.), 2012, *The Oxford Handbook of the Economics of Peace and Conflict*, Oxford University Press, New York.
- [21] Goldberg, Ian, 2007, Privacy-enhancing technologies for the internet III: Ten years later, in: Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis, Sabrina di Vimercati (eds.), *Digital Privacy, Theory, Technologies, and Practices*, Auerbach Publications, Boca Raton FL, Chapter 1, 3-18.
- [22] Hausken, Kjell, 2014, Choosing what to protect when attacker resources

and asset valuations are uncertain, *Operations Research and Decisions*, 3, 23-44.

- [23] Hausken, Kjell, 2017, Defense and attack for interdependent systems, *European Journal of Operational Research*, 256(2), 582-591.
- [24] Hausken, Kjell, and Vicki M. Bier, 2011, Defending against multiple different attackers, *European Journal of Operational Research*, 211(2), 370-384.
- [25] Herbst, Luisa, Kai A. Konrad, and Florian Morath, 2015, Endogenous group formation in experimental contests, *European Economic Review*, 74, 163-189.
- [26] Heurix, Johannes, Peter Zimmermann, Thomas Neubauer, and Stefan Fenz, 2015, A taxonomy for privacy enhancing technologies, *Computers & Security*, 53, 1-17.
- [27] Hillman, Arye L., and John G. Riley, 1989, Politically contestable rents and transfers, *Economics & Politics*, 1(1), 17-39.
- [28] Konrad, Kai A., 2009, *Strategy and Dynamics in Contests*, Oxford University Press, Oxford.
- [29] Kontos, Konstantinos, and Manolis Maragoudakis, 2016, Automated pool detection from satellite images using data mining techniques, *International Journal of Image Mining*, 2(2), 85-99.
- [30] Levitin, Gregory, Kjell Hausken, and Yuanshun Dai, 2014, Optimal defense with variable number of overarching and individual protections, *Reliability Engineering & System Safety*, 123, 81-90.
- [31] Levitin, Gregory, Kjell Hausken, and Hanoch Ben Haim, 2014, False targets in defending systems against two sequential attacks, *Military Operations Research*, 19(1), 19-35.

- [32] Montes, Rodrigo, Wilfried Sand-Zantman, and Tommaso Valletti, 2018, The value of personal information in markets with endogenous privacy, *Management Science*, <https://doi.org/10.1287/mnsc.2017.2989>.
- [33] Nitzan, Shmuel, 1991a, Collective rent dissipation, *Economic Journal*, 101(409), 1522-1534.
- [34] Nitzan, Shmuel, 1991b, Rent-seeking with non-identical sharing rules, *Public Choice*, 71(1-2), 43-50.
- [35] Richey, Michelle, Aparna Gonibeed, and M. N. Ravishankar, 2018, The perils and promises of self-disclosure on social media, *Information Systems Frontiers*, 20(3), SI 425-437.
- [36] Roth, Philip L., Philip Bobko, Chad H. Van Iddekinge, and Jason B. Thatcher, 2016, Social media in employee-selection-related decisions: A research agenda for uncharted territory, *Journal of Management*, 42(1), 269-298.
- [37] Shen, Yun, and Siani Pearson, 2011, Privacy enhancing technologies: A review, *HP Laboratories*, HPL-2011-113, 2739, 1-30.
- [38] Schipper, Burkhard C., and Hee Woo, 2017, Political awareness, microtargeting of voters, and negative electoral campaigning, *SSRN*: <https://ssrn.com/abstract=2039122>.
- [39] Tian, Feng, Tian Lan, Kuo-Ming Chao, Nick Godwin, Qinghua Zheng, Nazaraf Shah, and Fan Zhang, 2016, Mining suspicious tax evasion groups in big data, *IEEE Transactions on Knowledge and Data Engineering*, 28(10), 2651-2664.
- [40] Tullock, Gordon, 1967, The welfare costs of tariffs, monopolies, and theft, *Western Economic Journal*, 5(3), 225-232.

- [41] Tullock, Gordon, 1980, Efficient rent seeking, in: James M. Buchanan, Robert D. Tollison, and Gordon Tullock (eds.), *Toward a Theory of the Rent-seeking Society*, Texas A&M University Press, College Station, 97-112.
- [42] Uzialko, Adam C., 2018, Best online reputation management services 2018, *Business News Daily*, January 2, 2018 (<https://www.businessnewsdaily.com/7901-best-reputation-management-services.html>, accessed: August 09, 2018, 1926 GMT).
- [43] Vishwanath, Arun, Weiai Xu, and Zed Ngoh, 2018, How people protect their privacy on facebook: A cost-benefit view, *Journal of the Association for Information Science and Technology*, 69(5), 700-709.